Y 4.G 74/6: L 52/3

94th Congress
2d Session } JOINT COMMITTEE PRINT

94-2

LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S. 3418 (PUBLIC LAW 93-579)

SOURCE BOOK ON PRIVACY

COMMITTEE ON GOVERNMENT OPERATIONS
UNITED STATES SENATE

AND THE

COMMITTEE ON GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON GOVERNMENT INFORMATION
AND INDIVIDUAL RIGHTS

UNIVERSITY OF FLORIDA LIBRARIES
OCT 1976
DOCUMENTS DEPT.

SEPTEMBER 1976

Printed for the use of the Committee on Government Operations, United States Senate, and the Committee on Government Operations, House of Representatives

94th Congress
2d Session

JOINT COMMITTEE PRINT

LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974
S. 3418 (PUBLIC LAW 93-579)

SOURCE BOOK ON PRIVACY

COMMITTEE ON GOVERNMENT OPERATIONS
UNITED STATES SENATE

AND THE

COMMITTEE ON GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON GOVERNMENT INFORMATION
AND INDIVIDUAL RIGHTS



SEPTEMBER 1976

Printed for the use of the Committee on Government Operations, United States Senate, and the Committee on Government Operations, House of Representatives

U.S. GOVERNMENT PRINTING OFFICE
63-619 O WASHINGTON : 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $12.45

COMMITTEE ON GOVERNMENT OPERATIONS

ABRAHAM RIBICOFF, Connecticut, *Chairman*

JOHN L. McCLELLAN, Arkansas
HENRY M. JACKSON Washington
EDMUND S. MUSKIE, Maine
LEE METCALF, Montana
JAMES B. ALLEN, Alabama
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio

CHARLES H. PERCY, Illinois
JACOB K. JAVITS, New York
WILLIAM V. ROTH, JR., Delaware
BILL BROCK, Tennessee
LOWELL P. WEICKER, JR., Connecticut

RICHARD A. WEGMAN, *Chief Counsel and Staff Director*
PAUL HOFF, *Counsel*
PAUL L. LEVENTHAL, *Counsel*
ELI E. NOBLEMAN, *Counsel*
DAVID R. SCHAEFER, *Counsel*
MATTHEW SCHNEIDER, *Counsel*
CLAUDIA R. HIGGINS, *Assistant to the Majority*
JOHN B. CHILDERS, *Chief Counsel to the Minority*
BRIAN CONBOY, *Special Counsel to the Minority*
MARILYN A. HARRIS, *Chief Clerk*
ELIZABETH A. PREAST, *Assistant Chief Clerk*
HAROLD C. ANDERSON, *Staff Editor*

JAMES H. DAVIDSON, *Counsel, Subcommittee on Intergovernmental Relations*

COMMITTEE ON GOVERNMENT OPERATIONS

JACK BROOKS, Texas, *Chairman*

L. H. FOUNTAIN, North Carolina
JOHN E. MOSS, California
DANTE B. FASCELL, Florida
WILLIAM S. MOORHEAD, Pennsylvania
WM. J. RANDALL, Missouri
BENJAMN S. ROSENTHAL, New York
JIM WRIGHT, Texas
FERNAND J. ST GERMAIN, Rhode Island
FLOYD V. HICKS, Washington
DON FUQUA, Florida
JOHN CONYERS, JR., Michigan
BELLA S. ABZUG, New York
JAMES V. STANTON, Ohio
LEO J. RYAN, California
CARDISS COLLINS, Illinois
JOHN L. BURTON, California
RICHARDSON PREYER, North Carolina
ROBERT F. DRINAN, Massachusetts
EDWARD MEZVINSKY, Iowa
BARBARA JORDAN, Texas
GLENN ENGLISH, Oklahoma
ELLIOTT H. LEVITAS, Georgia
DAVID W. EVANS, Indiana
ANTHONY MOFFETT, Connecticut
ANDREW MAGUIRE, New Jersey
LES ASPIN, Wisconsin

FRANK HORTON, New York
JOHN N. ERLENBORN, Illinois
JOHN W. WYDLER, New York
CLARENCE J. BROWN, Ohio
GILBERT GUDE, Maryland
PAUL N. McCLOSKEY, JR., California
SAM STEIGER, Arizona
GARRY BROWN, Michigan
CHARLES THONE, Nebraska
ALAN STEELMAN, Texas
JOEL PRITCHARD, Washington
EDWIN B. FORSYTHE, New Jersey
ROBERT W. KASTEN, JR., Wisconsin
WILLIS D. GRADISON, JR., Ohio

WILLIAM M. JONES, *General Counsel*
JOHN E. MOORE, *Staff Administrator*
WILLIAM H. COPENHAVER, *Associate Counsel*
LYNNE HIGGINBOTHAM, *Clerk*
J. P. CARLSON, *Minority Counsel*

GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE

BELLA S. ABZUG, New York, *Chairwoman*

LEO J. RYAN, California
JOHN CONYERS, JR., Michigan
JOHN E. MOSS, California
MICHAEL HARRINGTON, Massachusetts
ANDREW MAGUIRE, New Jersey
ANTHONY MOFFETT, Connecticut

SAM STEIGER, Arizona
CLARENCE J. BROWN, Ohio
PAUL N. McCLOSKEY, JR., California

EX OFFICIO

JACK BROOKS, Texas

FRANK HORTON, New York

TIMOTHY H. INGRAM, *Staff Director*
ERIC L. HIRSCHHORN, *Counsel*
ROBERT S. FINK, *Professional Staff Member*
THEODORE J. JACOBS, *Professional Staff Member*
MARILYN HAFT, *Professional Staff Member*
ANITA WIESMAN, *Clerk*
MAURA FLAHERTY, *Secretary*

Digitized by the Internet Archive
in 2013

http://archive.org/details/ehisto00unit

PREFACE

It is a privilege to present to the Senate and to the general public this source book on the Privacy Act of 1974. That legislation represents a landmark achievement in securing for each citizen of the United States the right of privacy with respect to confidential information held by the Federal Government.

This legislation would not have become public law without the extraordinary dedication, ability, and leadership of Senator Sam J. Ervin, Jr., of North Carolina, who served as Chairman of the Committee on Government Operations in the 93d Congress.

For two decades, Senator Ervin was regarded by his colleagues in the Senate as a guardian and forceful exponent of the constitutional rights of our Nation's citizens. The hearings, reports, and legislation produced by the Subcommittee on Constitutional Rights of the Committee on Judiciary, which he also served as chairman, laid the groundwork for this first major privacy legislation.

The Bill of Rights guarantees to each American protections which we equate with specific rights of citizenship in a free society. This legislation is a major first step in a continuing effort to define the "penumbra" of privacy which emanates from specific guarantees in the Bill of Rights and which helps to give them life and substance as recognized in *Griswold* v. *Connecticut*.

This source book is an effort to bring together in one publication the legislative history which led to enactment of Public Law 93–579, the Privacy Act of 1974. In addition, it includes statements, articles, and certain reported cases which may help to shed light on the growing law of privacy.

It is hoped that this compilation of materials will be a useful reference for all people concerned with the Federal Government's role in the protection of privacy.

Sincerely,

ABRAHAM RIBICOFF, *Chairman*,
EDMUND S. MUSKIE.
CHARLES H. PERCY.

PREFACE

This source book on the Privacy Act of 1974 should be of assistance to government agencies charged with observing its mandates, and should be of help to private citizens in exercising their rights under this new law.

The Privacy Act is a law of fundamental importance. In addition to securing to each individual the right of access to files maintained by federal agencies, it also provides for the correction of inaccurate and outdated information in those files. The Act also places certain curbs on the random distribution of personal information, and requires that reasonable security safeguards be applied by agencies in the handling and storing of such data.

As with other landmark pieces of legislation, such as the Freedom of Information Act, when it was first passed in 1966, there is an initial period when education is needed to acquaint both government employees and citizens about the Act's requirements. The Privacy Act of 1974 is experiencing that situation now, and it is hoped that this publication will assist its implementation.

Sincerely,

JACK BROOKS,
Chairman,
Government Operations Committee.

BELLA S. ABZUG,
Chairwomen,
Government Information and Individual Rights Subcommittee.

WILLIAM MOORHEAD,
Former Chairman,
Foreign Operations and Government Information Subcommittee.

CONTENTS

Page

Prefaces ..... V, VII

CHAPTER I.—THE PRIVACY ACT: LEGISLATIVE HISTORY

Part One: The Major Bills

Senator Ervin introduces S. 3418 3
Text of S. 3418 9
Markup session transcript on S. 3418 29
S. 3418 as reported from the Committee on Government Operations 97
Senate Report No. 93-1183—Protecting Individual Privacy in Federal Gathering, Use, and Disclosure of Information 151
H.R. 16373 as introduced, August 12, 1974 239
H.R. 16373 as reported from the Committee on Government Operations 258
House Report No. 93-1416—Privacy Act of 1974 294
S. 3418 as passed by Senate, Nov. 21, 1974 and referred to House 334
H.R. 16373 as passed by the Senate, Nov. 22, 1974 375
S. 3418 as amended by House, Dec. 11, 1974 437
S. 3418 with Senate amendments to House amendments, Dec. 17, 1974 459
S. 3418 with House amendments to Senate amendments, Dec. 18, 1974 497
Public Law 93-579—The Privacy Act of 1974 501

Part Two: Additional Privacy Legislation

S. 1688—Civil Service Employees Right to Privacy 516
Senate Report 93-724 on S. 1688 536
S. 2542—Records Disclosure Privacy Act 584
S. 2810—Right to Privacy Act 591
S. 2963—Criminal Justice Information Control and Protection of Privacy Act 614
S. 3116—Mailing List Privacy Act 651
S. 3633—Government Data Bank Right to Privacy Act 654
H.R. 1281—Civil Service Employee's Right to Privacy Act 676
H.R. 7677—Civil Service Employees Right to Privacy Act 701
H.R. 12206—Records Disclosure Privacy Act 721
H.R. 13872—Records Disclosure Privacy Act 726
H.R. 14493—Federal Agency Information Practices Act 739

Part Three: Legislative Debate

SENATE ACTION—S. 3418

Senators Goldwater and Percy introduce an amendment to halt the spread of the social security number as a universal population identifier, September 19, 1974 759
Senate considers S. 3418 as reported by the Committee on Government Operations and passes it with amendments, November 21, 1974 763
Consideration of perfecting amendments 764
Memorandum explaining perfecting amendments 767
Executive branch views 772
Senator Percy's remarks on S. 3418 775
Senator Curtis' questions regarding the Bureau of the Census 781
Senator Muskie introduces amendment to enlarge mandate of the Privacy Protection Commission 783
Amendment introduced by Senator Nelson to establish a Joint Committee on Government Surveillance 787

Senate considers S. 3418 as reported by the Committee on Government Operations and passes it with amendments, Nov. 21, 1974—Continued
Page
Amendment introduced by Senator Goldwater to halt the spread of the social security number as a universal population identifier 804
Amendment introduced by Senator Weicker—Net Worth Disclosure Act 813
Senator Biden introduces an amendment relating to the Privacy Commission budgeting process 823
Rollcall vote on S. 3418 as amended 838
Senate considers H.R. 16373, substitutes text of S. 3418, November 22, 1974 838
Senate considers House substitute of text of H.R. 16373 to S. 3418 and adopts compromise amendments identical to those to be considered in the House 839
Senator Ervin submits an "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act," December 17, 1974 858
Staff memorandum in opposition to compromise on law enforcement provisions submitted by Senator Hruska 874
Senate considers and adopts three technical amendments passed by the House which further amend the Senate-House compromise amendments to S. 3418, December 18, 1974 878

HOUSE ACTION

House considers H.R. 16373, November 20, 1974 880
Perfecting amendments offered by Mr. Moorhead 907
Amendment offered by Mr. Erlenborn exempting civil service employment 908
Amendment offered by Mr. Fascell regarding civil remedies for agency failure to comply with the act 919
House continues consideration of H.R. 16373 and passes it with amendments, November 21, 1974 924
Amendment offered by Mr. Moorhead in compromise of positions on civil remedies provided against the Government 925
Amendment offered by Mr. Ichord to clarify position on law enforcement records 929
Amendment offered by Mr. Gude to clarify emergency situations which would allow disclsoure of information without prior consent 931
Amendment offered by Mr. Goldwater to place a moratorium on the use of the social security number 932
Amendment offered by Mr. Butler to allow disclosure pursuant to court order 936
Amendment offered by Mr. Butler to exempt from disclosure information compiled in reasonable anticipation of a civil action or proceeding 936
Amendment offered by Ms. Abzug to strike the exemption allowed for records maintained by the Central Intelligence Agency 938
Amendment offered by Mr. Ichord to exempt from disclosure certain investigatory material of investigating agencies in limited circumstances 944
Amendment offered by Mr. Gude to establish a Federal Private Commission 945
Amendment offered by Mr. Koch to require the Federal Register to publish a directory of Federal data banks 952
Amendment offered by Ms. Abzug to strike exemption allowed for Secret Service 953
Statement by the President endorsing H.R. 16373 956
Speeches by numerous members in general support of the act 959
Report of the Republican Task Force on Privacy 971
Final vote on passage of the bill 981
House considers S. 3418 and substitutes the text of H.R. 16373, December 11, 1974 984
House considers and adopts compromise amendments with three technical amendments. Congressman Moorhead submits an "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act," December 18, 1974 985

Part Four: Complementary Speeches and Materials

Page

Statement of the President upon the signing of the Privacy Act of 1974, January 1, 1975 1001
Statement of the President on the implementation of the Privacy Act of 1974, September 29, 1975 1002
Central Intelligence Agency comments on S. 3418 in a letter to Senator Ervin on September 26, 1974 1003
Address by the President on the "American Right of Privacy"—live on nationwide radio from the White House, February 23, 1974 1005
Senator Hart responds to President Nixon's radio broadcast on the Right of Privacy, March 7, 1974 1008

CHAPTER II.—DEVELOPMENTS SINCE ENACTMENT

OMB guidelines, July 1, 1975 1015
Transmittal memorandum No. 1, circular A–108, September 30, 1975 .. 1125
Supplement, November 21, 1975 1131
Congressional casework and the Privacy Act: Letter from Senators Ribicoff, Muskie, and Percy, Representatives Brooks and Abzug to colleagues, October 6, 1975 1134
Congressional Record insertion of February 15, 1976 1136
Department of Defense Privacy Board decision memorandum 76–1 1146
The Freedom of Information and Privacy Acts: Senator Kennedy's communication with the Department of Justice inserted in Congressional Record, October 9, 1975 1173

CHAPTER III.—EXPLANATORY ARTICLES AND CRITICISM OF THE ACT

Davidson, James H.:
The Privacy Act of 1974—Exceptions and Exemptions 1191
Cohen, Richard E.:
Protection of Citizens' Privacy Becomes Major Federal Concern, October 12, 1974 National Journal Reports 1195
New Privacy Law To Have Major Impact on Government Data, January 4, 1975 National Journal Reports 1208
Agencies Prepare Regulations for Implementing New Privacy Law, May 24, 1975 National Journal Reports 1211
Hulett, Privacy and the Freedom of Information Act, 27 Admin. L. Rev. 275 (1975) 1217
Large, Arlen J., "The Continuing Problem of Privacy," The Wall Street Journal, November 13, 1974 and "Congress Finishes Work on 'Privacy' Bill But Measure Has a Number of Loopholes," The Wall Street Journal, December 19, 1974 1237
Ervin, Sam J., Jr.:
"The First Amendment: A Living Thought in the Computer Age," from the Columbia Human Rights Review, vol. 4, No. 1 (1972) ... 1240
"Privacy and Government Investigations" Excerpts from the University of Illinois Law Forum, vol. 1971, No. 2 1261

CHAPTER IV.—CATEGORICAL BIBLIOGRAPHY

Selected bibliography of the rights of privacy and maintenance of Federal Records 1281

APPENDIXES

A. "Citizen Access to Records: A Guide to Federal Statutory Requirements," by Jerome Hanus, Government Division, Congressional Research Service, Library of Congress 1295
B. Excerpts from University of Michigan Law Review, Volume 73, "Increasing Protection of Citizen Privacy":
Introduction 1299
Constitutional Law of Privacy 1309
Statutory Protection Prior to the Privacy Act 1329
The Privacy Act of 1974 1335

	Page
C. Selected case law regarding the personal privacy exemption to the Freedom of Information Act and an Analysis	1373
Department of the Air Force v. *Rose*, —— U.S. ——, 44 U.S.L.W. 4503 (April 20, 1976)	1375
Rose v. *Department of the Air Force*, 495 F. 2d 261 (2d Cir. 1974)	1390
United States v. *Miller*, —— U.S. ——, 44 U.S.L.W. 4528 (April 21, 1976)	1400
Ditlow v. *Shultz*, 517 F.2d 166 (D.C. Cir. 1975)	1409
Wine Hobby USA v. *U.S. Internal Revenue Service*, 502 F.2d 133 (3d Cir. 1974)	1420
Rural Housing Alliance v. *U.S. Department of Agriculture*, 498 F.2d 73 (D.C. Cir. 1974)	1430
Robles v. *EPA*, 484 F.2d 843 (4th Cir. 1973)	1439
Getman v. *NLRB*, 450 F.2d 670 (D.C. Cir. 1971)	1444
D. Expungement of Records—*Chastain* v. *Kelley*, 510 F.2d 1232 (D.C. Cir. 1975)	1453

CHAPTER I

Legislative History of the Privacy Act of 1974

PART 1—THE MAJOR BILLS

[From the Congressional Record—Senate, May 1, 1974]

INTRODUCTORY REMARKS OF SENATOR SAM J. ERVIN, JR., ON S. 3418 [1]

[P. S6741]

ESTABLISHMENT OF A FEDERAL PRIVACY BOARD

Mr. ERVIN. Mr. President, with the concurrence of Mr. Percy and Mr. Muskie I introduce for reference to the Government Operations Committee a bill to establish a Federal Privacy Board, to oversee the gathering and disclosure of information concerning individuals, and to provide management systems in all Federal agencies, State and local governments, and other organizations.

Recent months have focused a great deal of attention, both in the Congress and with the public at large, on one of our most fundamental civil liberties—the right to privacy.

The Constitution creates a right to privacy which is designed to assure that the minds and hearts of Americans remain free. The bulwark of this constitutional principle is the first amendment. The first amendment was designed to protect the sanctity of the individual's private thoughts and beliefs. It protects the individual's right to free exercise of conscience; his right to assemble to petition the Government for redress of grievances; his right to associate peaceably with others of like mind in pursuit of a common goal; his right to speak freely what he believes; and his right to try to persuade others of the worth of his ideas.

The fourth amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In addition to the privacy of one's home and personal effects, the privacy of his person—or bodily integrity—and even his private telephone conversations are protected by the fourth amendment. The fifth amendment guarantees that an individual shall not be forced to divulge private information which might incriminate him. It also protects individual privacy by preventing unwarranted governmental intereference with the individual's person, personality, and property without due process of law.

The ninth amendment's reservation that "the enumeration in the Constitution of certain rights, shall not be construed to deny or dis-

[1] See p. 9.

parage others retained by the people" clearly shows that the Founding Fathers contemplated that certain basic individual rights not specifically mentioned in the Constitution—such as privacy—should nevertheless be safe from governmental interference.

The Supreme Court has held many aspects of individual privacy to be constitutionally protected. In recognizing that "specific guarantees in the Bill of Rights have penumbras formed by emanations from those guarantees that help give them life and substance" (*Griswold* v. *Connecticut*, 381 U.S. 479, 484), the Court has found that those penumbras protect the right to give and receive information, the right to family life and child-rearing according to one's conscience, the right to marriage, the right to procreation, the right to contraception, and the right to abortion.

All Americans can testify to the power of those protections of the individual's rights. The Constitution assures these rights to all citizens whether their exercise is pleasing to Government or not. And by the same token, it assures the individual the converse of these rights: the right not to speak what he believes, whether his silence is pleasing to Government or not; and his right not to act, not to associate, not to assemble, whether his inaction is pleasing to Government or not.

The right of every individual in America to privacy has been a matter of considerable concern to me over the years. It seems that now, as never before, the appetite of government and private organizations for information about individuals threatens to usurp the right to privacy which I have long felt to be among the most basic of our civil liberties as a free people.

If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.

Alexander Solzyhenitsyn, the Russian Nobel Prize winner, suggests how an all-knowing government dominates its citizens in his book "Cancer Ward:"

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber, banks, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

Perhaps it should come as no surprise that a Russian can master the words to describe the elusive concept we in America call personal

privacy. He understands, in a way which we cannot, the importance of being a free individual with certain inalienable rights, an individual secure in the knowledge that his thoughts and judgments are beyond the reach to the state or any man. He understands those concepts because he has no such security or rights but lives in a country where rights written into law are empty platitudes.

Privacy, like many of the other attributes of freedom, can be easiest appreciated when it no longer exists. A complacent citizenry only becomes outraged about its loss of integrity and individuality when the aggrandizement of power in the Government becomes excessive. By then, it may be too late. We should not have to conjure up 1984 or a Russian-style totalitarianism to justify protecting our liberties against Government encroachment. Nor should we wait until there is such a threat before we address this problem. Protecting against the loss of a little liberty is the best means of safeguarding ourselves against the loss of our freedom.

The protection of personal privacy is no easy task. It will require foresight and the ability to forecast the possible trends in information technology and the information policies of our Government and private organizations before they actually take their toll in widespread invasions of the personal privacy of large numbers of individual citizens. Congress must act before sophisticated new systems of information gathering and retention are developed, and before they produce widespread abuses. The peculiarity of new complex technologies is that once they go into operation, it is too late to correct our mistakes or supply our oversight.

Our Founding Fathers had that foresight when they wrote the Bill of Rights. The first, fourth and fifth amendments are among the most effective bulwarks to personal freedom conceived by the mind of man. Justice Brandeis in his classic dissent in the wiretapping case, *Olmstead* v. *United States*, 277 U.S. 438, 478 (1927), described with unsurpassed eloquence the importance of the right to privacy set out in the Constitution. These words do not go stale from repetition:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.

Government and private data collection on individuals is not a brand new phenomenon. The Federal Government has been collecting immense amounts of very sensitive information on individuals for decades. Income tax, social security, and census come to mind immediately. Various surveys by experts, private organizations such as the National Academy of Sciences, and a number of congressional committees have established the fact that the Federal Government stores massive amounts of information about all of us.

63-619 O - 76 - 2

Nevertheless, the effect on the right to privacy of massive information-gathering and dissemination through the use of sophisticated computer technology is just beginning to be realized. Rich or poor, male or female, whatever one's cultural style or religious or political views, each of us is subject to cumulative records being stored by a variety of Government agencies and private organizations.

One of the most obvious threats the computer poses to privacy comes in its ability to collect, store, and disseminate information without any subjective concern for human emotion and fallability.

Yet the increasing growth of information-gathering by Government and private organizations proceeds without any standards or procedures to regulate these organizations. It is because of this vacuum of authority that I am introducing, along with the very distinguished ranking minority member, Senator PERCY, this bill which is essential in order to preserve individual freedoms. We must act now to create safeguards against the present and potential abuse of information about people. I would like to provide a brief summary of its provisions.

THE FEDERAL PRIVACY BOARD

The bill establishes a Federal Privacy Board which shall have the primary function of overseeing the gathering, maintenance and disclosure of information concerning individuals by Federal agencies, State and local governments, and private organizations.

This Federal Privacy Board consists of five members, appointed by the President with the advice and consent of the Senate, not more than three of which are to be of the same political party. No member may engage in any other employment during his tenure.

In addition to its primary responsibility in enforcing the safeguards to personal privacy proscribed under section II of this bill, the Board is responsible for making an annual report to the President and to Congress, as well as publishing, on an annual basis, a descriptive directory of all information systems currently operating in the United States.

In order to carry out its functions, the Board is designated several specific powers. First, the Board shall have the power to compel, through subpena if necessary the production of any documents relating to an information system, either private or public.

Second, upon determination of a violation of any provisions of this act, the Board is authorized to issue cease and desist orders and to recommend the institution of either criminal or civil suits.

Third, the Board can conduct open public hearings on any petition for exemption from the provisions of section II of the act. Upon completion of its hearings, the Board will report its recommendation to the Congress.

SAFEGUARDS FOR PERSONAL PRIVACY IN INFORMATION SYSTEMS

The bill provides safeguards to personal privacy at all three stages of the information systems process: collection, maintenance, and dissemination of information.

COLLECTION OF INFORMATION

Under the provisions of the bill, information may be gathered by Federal agencies, State and local governments, or any private organizations only to accomplish the proper purpose of those agencies and organizations.

In gathering information, the individual must be the source of that information to the greatest extent possible; however, no individual may be forced to disclose any information not required by law, and he is to be informed of his right not to disclose.

The individual is to be notified of the existence of any information being maintained on him and the uses to which that information is being put.

No public or private organization may collect information on an individual's political or religious beliefs or affiliations unless specified by law.

A description of all information systems must be reported to the Federal Privacy Board on an annual basis.

MAINTENANCE

Restrictions on the maintenance of information systems used by Federal agencies, State and local governments, and other organizations include requirements that all information in these systems be accurate, complete, timely, and pertinent.

Any individual has the right to inspect the information maintained in a system relating to him with the exception of medical records. He has the right to know the nature of the source and the recipients of that information.

The individual also has the right to challenge any information on the basis of its accuracy, completeness, timeliness, pertinence, or necessity. Upon receipt of any challenge to its information by an individual, an organization must: First, investigate and record the current status of such information; second, purge any information that is found to be incomplete, not pertinent, not timely, not necessary to be maintained, or that can no longer be verified.

If the investigation does not solve the dispute, the individual may insert a statement, not in excess of 200 words, in his own defense, and he may appeal to the Federal Privacy Board.

DISSEMINATION

The bill places strict restrictions on the dissemination of information in personal information systems, both private and public.

All information systems must request permission from the individual before disseminating any information to any person or organization not having regular, authorized access to the information system.

Organizations maintaining information systems are required to keep an accurate list of all persons having access to the information including but not limited to those having access on a regular basis.

Federal agencies are specifically restricted in disseminating information only to authorized employees of Federal agencies.

SOCIAL SECURITY NUMBERS

The omnibus privacy bill makes it unlawful for any organization to require an individual to disclose or furnish his social security number unless specifically required by law.

MAILING LISTS

The bill also provides for the removal of any name and address from a mailing list upon the written request of the individual.

REMEDIES

The remedies provided under this act include both criminal and civil sanctions.

The act provides for a criminal liability of up to $10,000 or 5 years in prison, or both, for any violation of the act.

In addition, the act provides that the Attorney General, upon the recommendation of the Federal Privacy Board, or an aggrieved individual, may file a civil suit in the appropriate district court.

EXEMPTIONS

Certain types of information are exempted from coverage of this act. Those information systems exempted include: any information maintained by a Federal agency and determined to be vital to national defense; criminal investigatory files of Federal, State or local law enforcement agencies; and any information maintained by the press or news media—except that information related to the employees of such organizations.

CONCLUSION

Mr. President, this bill provides a method whereby the Congress can guarantee that the right of every American to be let alone will be maintained. I encourage every Senator to support this important piece of legislation.

PART 1—MAJOR BILLS

93D CONGRESS
2D SESSION

S. 3418

IN THE SENATE OF THE UNITED STATES

MAY 1, 1974

Mr. ERVIN (for himself, Mr. PERCY, and Mr. MUSKIE) introduced the following bill; which was read twice and referred to the Committee on Government Operations

A BILL

To establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State, and local governments, and other organizations regarding such information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I—FEDERAL PRIVACY BOARD

ESTABLISHMENT OF BOARD

SEC. 101. (a) There is established in the executive branch of the Government the Federal Privacy Board which shall be composed of five members who shall be appointed by the President by and with the advice and consent of the

Senate from among members of the public at large who are not officers or employees of the United States. Not more than three of the members of the Board shall be adherents of the same political party.

(b) The Chairman of the Board shall be elected by the members of the Board every two years.

(c) Each member of the Board shall be compensated at the rate provided for GS–18 under section 5332 of title 5 of the United States Code.

(d) Members of the Board shall be appointed for a term of three years. No member may serve more than two terms.

(e) Vacancies in the membership of the Board shall be filled in the same manner in which the original appointment was made.

(f) Vacancies in the membership of the Board, as long as there are three members in office, shall not impair the power of the Board to execute the functions of the Board. Three members of the Board shall constitute a quorum for the transaction of business.

(g) Members of the Board shall not engage in any other employment during their tenure as members of the Board.

FUNCTIONS OF THE BOARD

SEC. 102. The Board shall—

(1) publish an annual Data Base Directory of the United States containing the name and characteristics of each personal information system;

(2) consult with the heads of appropriate departments, agencies, and instrumentalities of the Government in accordance with section 103(5) of this Act;

(3) make rules to assure compliance with title II of this Act; and

(4) perform or cause to be performed such research activities as may become necessary to implement title II of this Act, and to assist organizations in complying with the requirements of such title.

POWERS OF THE BOARD

SEC. 103. (a) The Board is authorized—

(1) to be granted admission at reasonable hours to premises where any information system is kept or where computers or equipment or recordings for automatic data processing are kept, and may, by subpena, compel the production of documents relating to such information system or such processing as is necessary to carry out its functions, except that the production of personal information shall not be compelled without the prior consent of the data subject to which it pertains;

(2) upon the determination of a violation of any provision of this Act or regulation promulgated under this Act, to, after opportunity for a hearing, order the organization violating such provision to cease and desist such violation;

(3) to delegate its authority under this title, with respect to information systems within a State or the District of Columbia, to such State or District, during such period of time as the Board remains satisfied that the authority established by such State or District to carry out the requirements of this Act in such State is satisfactorily enforcing those provisions;

(4) to conduct open, public hearings on all petitions for exceptions or exemptions from provisions, application, or jurisdiction of this Act, except that the Board shall not have authority to make such exceptions or exemptions but shall submit appropriate reports and recommendations to Congress; and

(5) to the fullest extent practicable, to consult with the heads of appropriate departments, agencies, and instrumentalities of the Government in carrying out the functions of the Board under this Act.

(b) The Board may procure such temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed $100 a day for individuals.

REPORTS

SEC. 104. The Board shall report, annually, on its activities to the Congress and the President.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, STATISTICAL-REPORTING AND RESEARCH PURPOSES

SEC. 201. (a) Any Federal agency, State or local government, or any other organization maintaining an information system that includes personal information shall—

(1) collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization;

(2) collect information to the greatest extent possible from the data subject directly;

(3) establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

(4) maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

(5) make no dissemination to another system without (A) specifying requirements for security and the use of information exclusively for the purposes set forth in the notice required under subsection (c) including limitations on access thereto, and (B) determining that

the conditions of transfer provide substantial assurance that those requirements and limitations will be observed;

(6) transfer no personal information beyond the jurisdiction of the United States without specific authorization from the data subject or pursuant to a treaty or executive agreement in force guaranteeing that any foreign government or organization receiving personal information will comply with the applicable provisions of this Act with respect to such information;

(7) afford any data subject of a foreign nationality, whether residing in the United States or not, the same rights under this Act as are afforded to citizens of the United States;

(8) maintain a list of all persons having regular access to personal information in the information system;

(9) maintain a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority;

(10) take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information con-

tained therein, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance;

(11) establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;

(12) comply with the written request of any individual who receives a communication in the mails, over the telephone, or in person from a commercial organization, who believes that the name or address or both, of such individual is available because of its inclusion on a mailing list, to remove such name or address, or both, from such list; and

(13) collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used or disseminated in or by any information system operated by any governmental agency, unless authorized by law.

(b) (1) Any such organization maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of other organizations, shall—

(A) make available to any data subject or group (without revealing trade secrets) methodology and materials necessary to validate statistical analyses, and

(B) make no materials available for independent analysis without guarantees that no personal information will be used in a way that might prejudice judgments about any data subject.

(2) No Federal agency shall—

(A) require any individual to disclose for statistical purposes any personal information unless such disclosure is required by law, and such individual is informed of such requirement;

(B) request any individual to voluntarily disclose personal information unless such request is specifically authorized by law, and the individual is advised that such disclosure is voluntary;

(C) make available to any person, other than an authorized officer or employee of a Federal agency, any statistical study or reports or other compilation of information derived by mechanical or electronical means from any file containing personal information, or any manual or computer material relating thereto, except those prepared, published, and made available for general public use; or

(D) publish statistics of taxpayer income classified, in whole or in part, on the basis of a coding system for the delivery of mail.

(c) Any such organization maintaining or proposing to establish an information system for personal information shall—

(1) give notice of the existence and character of each existing system once a year to the Federal Privacy Board;

(2) give public notice of the existence and character of each existing system each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations in local or regional printed media likely to bring attention to the existence of the records to data subjects;

(3) publish such annual notices for all its existing systems simultaneously;

(4) in the case of a new system, or the substantial modification of an existing system, shall give public notice and notice to the Federal Privacy Board within a reasonable time but in no case less than three months, in advance of the initiation or modification to assure individuals who may be affected by its operation a reasonable opportunity to comment; and

(5) assure that public notice given under this subsection specifies the following:

(A) the name of the system;

(B) the general purposes of the system;

(C) the categories of personal information and approximate number of persons on whom information is maintained;

(D) the categories of information maintained, confidentiality requirements, and access controls;

(E) the organization's policies and practices regarding information storage, duration of retention of information, and purging of such information;

(F) the categories of information sources;

(G) a description of types of use made of information including all classes of users and the organizational relationships among them;

(H) the procedures whereby an individual may (i) be informed if he is the subject of information in the system, (ii) gain access to such information, and (iii) contest the accuracy, completeness, timeliness, pertinence, and the necessity for retention of such information;

(I) the procedures whereby an individual or group can gain access to the information system used for statistical reporting or research in order to subject them to independent analysis; and

(J) the business address and telephone number of the person immediately responsible for the system.

(d) Any such organization maintaining personal information shall—

(1) inform any individual asked to supply personal information whether such individual is required by law, or may refuse, to supply the information requested, and also of any specific consequences which are known to the organization, of providing or not providing such information;

(2) request permission of a data subject to disseminate part or all of such information to another organization or system not having regular access authority, and indicate the use for which such information is intended, and the specific consequences for the individual, which are known to the organization, of providing or not providing such permission;

(3) upon request and proper identification of any individual who is a data subject, grant such individual the right to inspect, in a form comprehensible to such individual—

(A) all personal information about that individual except that, in the case of medical information, such information shall, upon written authorization, be given to a physician designated by the individual;

(B) the nature of the sources of the information; and

(C) the recipients of personal information about such individual including the identity of all persons and organizations involved and their relationship to the system when not having regular access authority;

(4) at a minimum, make disclosures which are required by this Act to individuals who are data subjects—

(A) during normal business hours;

(B) in person, if the data subject appears in person and furnishes proper identification, or by mail, if the data subject has made a written request, with proper identification, at reasonable standard charges for document search and duplication; and

(C) permit the data subject to be accompanied by one person of his choosing, who must furnish reasonable identification, except that an organization may require the data subject to furnish a written statement granting permission to the organization to discuss that individual's file in such person's presence;

(5) upon receipt of notice from any individual who is a data subject, that such individual wishes to chal-

lenge, correct, or explain information about him in such system—

(A) investigate and record the current status of such personal information;

(B) purge any such information that is found to be incomplete, inaccurate, not pertinent, not timely nor necessary to be retained, or can no longer be verified;

(C) accept and include in the record of such information, if the investigation does not resolve the dispute, any statement (not more than two hundred words in length) provided by such individual setting forth his position on such disputed information;

(D) in any subsequent dissemination or use of disputed information, clearly note that such information is disputed and supply the statement of such individual together with such information;

(E) make clear and conspicuous disclosure to such individual of his right to make a request under this paragraph;

(F) at the request of such individual, following any correction or purging of personal information, furnish to past recipients of such information notifi-

cation that the item has been purged or corrected; and

(G) in the case of a failure to resolve a dispute, advise such individual of his right to request the assistance of the Federal Privacy Board.

(e) Each such organization maintaining a personal information system on the date of the enactment of this Act shall notify by mail each data subject of the fact not later than two years following the date of enactment of this Act, at the last known address of the subject. Such notice shall—

(1) describe the type of information held in such system or systems, expected uses allowed or contemplated; and

(2) provide the name and full address of the place where the data subject may obtain personal information pertaining to him, and in the system.

(f) Data subjects of archival-type inactive files, records, or reports shall be notified by mail of the reactivation, accessing, or reaccessing of such files, records, or reports not later than six months after the date of the enactment of this Act.

(g) The requirements of subsections (a) (3) and (4) and subsections (c) and (d) (1) and (2) of this section shall not apply to any organization that (1) maintains an information system that disseminates statistical reports or

research findings based on personal information drawn from the system, or from systems of other organizations, (2) purges the names, personal numbers, or other identifying particulars of individuals, and (3) certifies to the Federal Privacy Board that no inferences may be drawn about any individual.

EXEMPTIONS

SEC. 202. The provisions of this title shall not apply to personal information systems—

(1) to the extent that information in such systems is maintained by a Federal agency, and the head of that agency determines that the release of the information would seriously damage national defense;

(2) which are part of active criminal investigatory files compiled by Federal, State, or local law enforcement organizations, except where such files have been maintained for a period longer than is necessary to commence criminal prosecution; or

(3) maintained by the press and news media, except information relating to employees of such organizations.

USE OF SOCIAL SECURITY NUMBER

SEC. 203. It shall be unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any

business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual (except to the extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program established under title II of the Social Security Act) in whole or in part because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by law.

TITLE III—MISCELLANEOUS

DEFINITIONS

SEC. 301. As used in this Act—

(1) the term "Board" means the Federal Privacy Board;

(2) the term "information system" means the total components and operations of a recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars;

(3) the term "personal information" means all information that describes, locates or indexes anything about an individual including his education, financial transactions, medical history, criminal, or employment

record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

(4) the term "data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system;

(5) the term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means;

(6) the term "organization" means any Federal agency; the government of the District of Columbia; any authority of any State, local government, or other jurisdiction; any public or private entity engaged in business for profit, as relates to that business;

(7) the term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization; and

(8) the term "Federal agency" means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof.

TRADE SECRETS

SEC. 302. In connection with any dispute over the application of any provision of this Act, no organization shall reveal any personal information or any professional, proprietary, or business secrets; except as is required under this Act. All disclosures so required shall be regarded as confidential by those to whom they are made.

CRIMINAL PENALTY

SEC. 303. Any organization or responsible officer of an organization who willfully—

(1) keeps an information system without having notified the Federal Privacy Board; or

(2) issues personal information in violation of this Act;

shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 304. (a) The Attorney General of the United States, on the advice of the Federal Privacy Board, or any aggrieved person, may bring an action in the appropriate United States district court against any person who has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this Act or rules of the Federal Privacy Board, to enjoin such acts or practices.

(b) Any person who violates the provisions of this Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

(1) any actual damages sustained by an individual;

(2) punitive damages where appropriate;

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

The United States consents to be sued under this section without limitation on the amount in controversy.

JURISDICTION OF DISTRICT COURTS

SEC. 305. The district courts of the United States have jurisdiction to enforce any subpena or order issued by the Federal Privacy Board under sections 102 or 103, respectively, of this Act.

RIGHT OF ACTION

SEC. 306. (a) Any individual who is denied access to information required to be disclosed under the provisions of this Act is entitled to judicial review of the grounds for such denial.

(b) The district courts of the United States have jurisdiction to hear and determine civil actions brought under subsection (a) of this section.

EFFECTIVE DATE

SEC. 307. This Act shall take effect one year after the date of its enactment.

AUTHORIZATION OF APPROPRIATIONS

SEC. 308. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.

MARK-UP SESSION

S. 3418

TO CREATE A FEDERAL PRIVACY COMMISSION

- - -

TUESDAY, AUGUST 20, 1974

- - -

United States Senate,

Committee on Government Operations,

Washington, D. C.

The committee met at 3:00 p.m., pursuant to call, in room S-146, The Capitol, Hon. Sam J. Ervin, Jr. (chairman of the committee) presiding.

Present: Senators Ervin, Jackson, Muskie, Allen, Chiles, Nunn, Huddleston, Percy, Javits, Roth and Brock.

Staff Present: Robert Bland Smith, Jr., Chief Counsel and Staff Director; Marcia MacNaughton, Consultant, Mrs. Gay Holliday, Staff Member; Richard Casad, Investigator, Permanent Subcommittee on Investigations.

The Chairman. It takes a quorum to report out a bill. We have a quorum here. We may have difficulty getting a quorum later, so I would like to move that we report the bill favorably subject to such amendments as may be adopted by the six members in case we fall down to six.

Senator Jackson. I second that motion.

Senator Javits. So do I.

Senator Brock. Mr. Chairman, there are some questions that need to be discussed on the bill. I am not sure what this means in a parliamentary sense but, for example, I have a very serious expression of concern from the SEC and I don't know whether that has been responded to by the committee, or whether we have written comments. At least I haven't seen them.

Senator Javits. If you would yield, why don't you vote no on this vote and -- rather, vote aye -- and then you can move to reconsider.

Senator Roth. Mr. Chairman, I think that establishes a very bad precedent. I think if the legislation is important, we should be able to get a quorum to finally pass it out. It is grounds for raising the issue on the Senate floor. I am just generally opposed to the proposition that any of us should put our stamp of endorsement or otherwise until we know -- I support it.

The Chairman. I will withdraw the motion.

Senator Javits. I tried to help.

Senator Percy. I think it should be noted, Senator Brock, on the question of SEC, staff has discussed with SEC certain reservations that they have and assured them that we can work those out and that they can be worked out to our mutual satisfaction.

Obviously, the whole intent and purpose of sending it there was to appraise and analyze what objections they might

have. We have not heard any that could not be accommodated.

Senator Brock. I haven't gotten any written response from the SEC. To the best of my knowledge, the committte has none. If it is true that the bill would, as they say, prohibit them from carrying out their own statutory responsibilities, then I think it would ill behoove us to move until we have a specific written response from them so we can incorporate such modifications as we deem necessary, but I don't think it is the intent of this bill to hamper the SEC in any sense. That is one of our better regulatory or supervisory agencies.

I just got a call from one of the commissioners who was extremely perturbed over the content of the bill. They had no time at all to prepare any response, and I question whether we ought to act without --

The Chairman. The OMB made a response on behalf of the entire Executive Branch of the government --

Senator Brock. You have been sort of critical of OMB responding on behalf of the whole government before.

The Chairman. Yes.

Senator Brock. Now you are going to say it is okay?

The Chairman. The SEC has known about the bill. It has had communications with members of the staff and members of this committee. I don't know that we could very well postpone until we hear from SEC. They know our address of the committee. They have had plenty of chance to respond.

Now we have got something here.

Senator Jackson. From the SEC.

The Chairman. We can certainly consider the amendments to the bill.

Senator Brock. Okay. This says they only recieved your letter yesterday and Committee Print 4. They have not even seen 5.

Senator Chiles. I doubt very seriously that all the agencies see all the Committee Prints, 4, 5, 6 or whatever goes through.

Senator Brock. No, but I think it is a practice of the Congress, Martin, when there is a sensitive agency who is according to their interpretation directly affected by the law to be very sure that we take into consideration their views. We don't have to agree with them. But here they say they endorse the concept of the bill, but they question apparently whether or not it would not impinge upon their ability to protect the regulatory authority that they have.

Senator Percy. Mr. Chairman, if I might be recognized, I think the important part of Garrett's letter is the last paragraph. It is terribly important. It says, "Notwithstanding our difficulties with the present version of S. 3418, this Commission strongly endorses the concept of personal privacy which we believe underlies Confidential Committee Print No. 4.

"No agency of the Government should be permitted to abuse

personal or confidential information, and this Commission has steadfastly adhered to such a standard over the 40 years of its existence, and we are proud of our record in that regard.

"We would be delighted to work with the Committee to effect an appropriate restructuring of Confidential Committee Print No. 4 so that it might both achieve the laudable purpose of protecting personal privacy while, at the same time, permit lawful government regulatory or law enforcement conduct.

"We also stand ready to furnish you with more detailed comments on our objections on Confidential Committee Print No. 4 of S. 3418 if you should so desire."

I think the question before the committee then is whether or not it is the feeling of the members that we could work this out at the staff level, consulting with committee members as need b, and being able to report out a completely acceptable bill, or whether we should just try to delay this until we have completed every last comma, dash, and dot and put it in that form.

I think we have a great deal of confidence in the committee. It could be carried out by the staff during the recess, and we wouldn't lose all that period of time.

From the Minority standpoint, we would certainly seek to counsel the chairman on it.

Senator Brock. I have been a supporter of the legislation, as you know. And I would very much like to see legislation

passed. I just don't want to do something that does not achieve our desired result.

The Chairman. I think the SEC is aware of the fact that the bill has been pending, it is aware that the President came out for a privacy bill. There has been a lot of discussion in the newspapers about it. We can't wait and let Congress be regulated by the delays that SEC may wish.

Senator Jackson. Might I ask a question, Mr. Chairman?

Do we have amendments from the SEC?

Senator Percy. No.

Senator Brock. They say, to read further in their letter - Chuck read the last paragraph. I think the next to the last paragraph is of more concern to me. They just got, as of yesterday, the Committee Print in which the new language bothers them.

"While time does not now permit a detailed exposition of the numerous ways in which Confidential Committee Print No. 4 apparently would impede and impair our ability to fulfill our statutory functions, I think it should be pointed out that much of the enforcement work handled by this Commission, which has served to protect public investors and maintain the honesty, integrity, fairness and efficiency of our securities markets, would either be subject to serious limitations or require the significant, curtailment of a number of our activities."

That is a pretty serious charge.

The Chairman. It is, but if they think it is so serious, they ought to be down here on it. They testified before the House committee.

Senator Brock. Yes, and the language has been modified. I don't know that they have had an opportunity for hearing since then.

The Chairman. They haven't asked for a hearing before this committee.

This bill has been pending here since May, and this is June, July and August, and it seems like the SEC is sure travelling on leaden feet if they have any concern about this bill.

Senator Brock. I am not trying to defend the SEC. I am trying to defend the quality of our work rather than quantity. There is a distinction. I don't know what the problem is. If there is a serious problem, it ought to be considered.

Senator Jackson. What concerns me is all we have are conclusions in this letter. They have a copy of Committee Print No. 4. They refer to that, but they don't state wherein they object. It is a general pleading without providing a bill of particulars and I should think, as I understand it, they have had the original bills, they have had the other Prints, but what confuses me is just what is their specific position regarding the kind of language that should be in any bill to properly protect what they consider to be their responsibility.

Senator Brock. That is the very question I am asking.

Senator Jackson. How do you deal with a piece of paper like this except reopen the hearings? That is what it amounts to.

The Chairman. They were diligent enough to contact the House committee on the sixth of May. My understanding is that it is rumored that the SEC is split down the middle of this bill. Some of them want it and some don't. They can't get a unified position to state to this committee. They could have communicated with us.

Senator Huddleston. In the absence of any specific suggestion, wouldn't it be appropriate to report the bill out? It is always subject to amendment on the floor if somebody could come with some language to improve the bill.

Senator Brock. The problem that I have with that is that I have been a very ardent supporter of the legislation, and it would put me in the position under the circumstances of feeling almost compelled to oppose reporting the bill until I have the facts on hand on which to make a decision. I don't know what changes in Committee Print No. 4 apparently bothered the SEC. I would like the specific information that the Senator from Washington seeks on which to make my own judgment.

I just don't know. I am reluctant to prod them into action that would be ill-advised.

Senator Jackson. Could someone get on the phone and ask them if they have an amendment?

I read this letter and it is no guide at all. This thing has been pending all these months. They must be able to identify, irrespective of this bill, the specific areas, and you are quite right, the next to the last paragraph goes to the heart of it on page 2. It says: "While time does not now permit a detailed exposition of the numerous ways in which Confidential Committee Print No. 4 apparently would impede and impair our ability to fulfill our statutory functions, I think it should be pointed out that much of the enforcement work handled by this Commission, which has served to protect public investors and maintain the honesty, integrity, fairness and efficiency of our securities markets, would either be subject to serious limitations or require the significant, curtailment of a number of our activities."

My question is: Wherein does that possibility exist? They just state the general conclusions.

Senator Roth. Mr. Chairman --

Senator Jackson. If this is that serious, I would think regardless of Committee Print 1, 2, 3, 4, 5, 6 or 7, they ought to be able to provide some statutory language that would properly cover their responsibility.

I can see some problems, but I get the same information that the Commission is split, and they can't agree to statutory language. I suggest that we defer this and someone talk to the chairman on the phone and find out what is the situation. This

WARD & PAUL
410 First Street, S.E., Washington, D.C. 20003

is sort of a confession in avoidance.

Senator Roth. Mr. Chairman, if we are going to take this to the Senate floor and they raise these same objections, we are going to be in a difficult position if we don't know what they are or the seriousness of their intent.

I am anxious to get this legislation out and adopted. I am not quite sure that I understand the problems of the time frame. If we do report it out today, are we going to take it up this week? Will that come up on the Senate floor this week?

Senator Percy. Not until September.

Senator Roth. There are some problems on the House side. It looks as if somebody is trying to dictate to us. We have some time to still report it out this week. I think Senator Jackson's suggestion is a good one, that we ought to call or have someone call on behalf of the committee.

Senator Percy. I wonder if I can make a motion and see, Senator Roth, whether it might not be acceptable.

Mr. Chairman, I would like to move that we report the bill out subject to an understanding that there would be a committee amendment or a series of committee amendments offered that would fully take into account objections, any objections, that come in that we feel need to be accommodated and that those would be offered as a series of committee amendments at the same time that the bill has been offered on the floor.

The Chairman. Well, we might not be able to agree on the

amendments. I understand the Executive Branch, the President of the United States was for privacy. I understand they designated OMB to represent all the agencies of the Government, and if SEC could inform the House on the sixth day of May on their opinion about the House bill, I don't see why they should travel along on some leaden feet.

Senator Percy. On the other hand, if they have perfectly legitimate objections that we can accommodate, and from the preliminary talks that staff has had, that seems to be possible, then why not make that provision because it at least accommodates those who have raised the issue.

This letter is certainly not a totally satisfactory answer. We could have an indication today by roll call vote about how we would feel about following this procedure. It has been around a long time. The session is getting short now.

The Chairman. I have been informed that the SEC advised the staff that they would have somebody here today. Is anybody here representing the SEC?

Senator Jackson. Are they outside?

Senator Percy. Take a look in the closets.

Senator Brock. Mr. Chairman, while we are trying to find out --

Senator Percy. Is there a second to the motion?

Senator Jackson. The only question is on this point, I would support it, but I think if Senators have reservations

and that has been expressed by Senator Brock and Senator Roth, maybe the wise course would be to start right through these amendments and see if we can't wrap up as much as possible here this afternoon and then act?

Senator Brock. That is what I was going to suggest. I would support Senator Percy's motion. This is what we had to do over in the Interior Committee to get near the end of the session. I don't like the practice, but realistically we can't maintain quorums. We have been reporting the subject to whatever action the committee may take on amendments, and then if any Senator raises any serious question, I have always moved to reconsider, but it is just the pragmatic problem of -- we don't have a quorum now.

Senator Roth. Mr. Chairman --

The Chairman. We have one over quorum.

Senator Jackson. I am sorry.

Senator Roth. If I understand Senator Percy's proposal, it was that we go ahead and report it out in its present form subject to the agreement that the considerations of the SEC would be considered at a later meeting, is that correct?

Senator Jackson. All amendments.

Senator Percy. All amendments. We would subsequently report the bill out with committee amendments to be considered at the same time, but at least it takes advantage of the fact that we have nine Senators in the room at the present moment,

and it is hard to get them here. As long as we are in agreement in principle that this is a good bill, but there are some details that have to be worked out, I think we can do that.

Senator Nunn. Are we going to stay and work out these details now, or are we going to --

Senator Percy. I am willing to stay right now. What we are concerned about is losing a quorum. I have to meet Senators Mansfield and Ribicoff on the floor to work out the next cloture position.

Senator Brock. Are you going to try again?

Senator Percy. It was supposed to be five minutes from now. Is there a second?

Senator Jackson. I second the motion.

The Chairman. Is there any discussion?

Senator Nunn. Let me make sure what this motion is. Are we going to report this out without any amendments being considered?

Senator Jackson. It is ordered reported out subject to the adoption of committee amendments which would require a quorum as I understand it, Mr. Chairman --

Senator Nunn. Subject to the adoption when? A meeting of this committee or on the floor?

Senator Percy. Just stay right now. We only require six instead of nine.

Senator Roth. Mr. Chairman, I would just like to repeat

that I think it makes a very bad precedent. If you are going to have credibility in the government, to have a committee adopt a bill that they don't even know what it is finally going to include is not sound procedure.

If this is important legislation, it is not that difficult to get a quorum here.

Senator Brock. We could have passed a couple of amendments if we go ahead and do it. Why don't we take the amendments up one by one. Let us vote as fast as we can.

Senator Nunn. This is an extremely important bill. I am in favor of it. It has been drastically improved by the staff work. The first bill I saw was broad enough to cover the corner grocery store in the smallest town in North Carolina or Georgia. It has been improved by the staff product. It is much better.

The Senators have not had a chance to focus on this. That does not mean I am in favor of it because I am. I think we ought to focus on this. It is much, much broader now than many people think. A lot of alternatives and a lot of hypothetical things that have not been considered could happen. I would be reluctant to vote on it without going through some discussion.

Senator Percy. I withdraw my motion. I suggest that we proceed on the amendments.

Senator Jackson. When Senator Percy comes back, I have a supplemental suggestion.

Senator Brock. Are we taking up Committee Print No. 4 or

5?

The Chairman. Let us start with the bill and go through it as far as we can.

Senator Brock. Committee Print No. 5, is that the one we are taking up?

The Chairman. Confidential Committee Print No. 5.

Are there any amendments to Title I which starts on page 1 and ends on page 13?

Does anyone have any amendments under Title I?

Senator Nunn. I would like to direct a question for the intent on page 6, subsection (c), beginning on line 14 where it says, "such report shall not proceed to establish or modify any such data bank or information system for a period of sixty days from the date of receipt of notice from the Commission that such data bank or system does not comply with such standards."

I assume that means that once the Commission says to the Federal Agency there is something wrong, this breaches our policy, that they can't act for 60 days.

Is it also their intention during that period of time that Congress also will be notified so that action can be taken here if we deemed it necessary?

Otherwise, you have got just a 60-day period and it will go into effect. I am not sure of the meaning, maybe it will come from somewhere else.

The Chairman. The Commission is to report to Congress

within a 60-day period.

Senator Nunn. Is that another section? It is not in that section. I would think that would be the intent, maybe it is somewhere else.

The Chairman. It says for a period of 60 days from date of receipt of the notice from the Commission that such data bank or system does not comply with such standards.

Senator Nunn. It the agencies proposed a new information system, and the Commission served notice that it breached some regulation of the agency, then the agency can't proceed for 60 days once they receive that notice, but my question is: Is there any provision in the bill that provides a corresponding notice to Congress so that we would be able to take action, otherwise, we would just have a notice to an agency saying that it defied the rules and nothing would happen, and it would go into effect after 60 days.

The Chairman. It says: "After receipt of any report required under subsection (b), if the Commission determines and report to the Congress that a proposal to establish or modify a data bank or information system does not comply with the standards established by or pursuant to this Act, the Federal agency submitting such report shall not proceed to establish or modify" --

Senator Nunn. I see. Okay. My question then becomes this: Is it envisoined the Congress then would have to pass a

law to prohibit that?

The Chairman. No, not necessarily. If the Federal agents do not proceed, it gives 60 days for any appropriation action to be taken.

Senator Nunn. But then they could proceed if there was no action taken. They could go ahead and establish a faulty system?

The Chairman. There are just some technical amendments to Title I which has been prepared. They don't change the substance.

The staff has been in contact with the gentleman in charge of privacy for the Administration, Senator Brock, and he says the OMB speaks for the Administration with respect to this bill.

Senator Brock. It is a noble endeavor, but I still don't accept it. I still want to hear from the SEC, Mr. Chairman. I think thta is only fair.

Senator Chiles. I thought this was going to be an open Administration. Is Mr. Ash still reigning?

Senator Brock. It sounds like it. With Sam Ervin behind him, he may be in good shape.

The Chairman. So far as privacy, OMB speaks for the Administration and SEC has proposed no amendments. I don't know how we can get the SEC to respond.

Senator Brock. Have you asked them?

The Chairman. I haven't. They are supposed to have an

observer here today. I don't know how Congress can put off its work for SEC to communicate to us as to what their desires are.

Senator Brock. Why don't we proceed with the amendments, Mr. Chairman.

The Chairman. There are a number of amendments to Title I, on page 2, line 5, strike out "the areas of" and insert in lieu thereof "any of the following areas:".

On page 3, line 24, strike out "Chairman" and insert in lieu thereof "members".

On page 4, line 1, strike out "during his tenure as Chairman" and insert in lieu thereof "during their tenure as members".

Senator Jackson. Mr. Chairman, might I make a suggestion? If all of the amendments we have on here, I think they are in the files, aren't they -- if the technical amendments are purely technical and do not change substance, with that assumption, I would suggest that a motion be in order to treat them en block and adopt them, and if there is any substantive change as a result of that, we can go back and correct it and I so move.

Senator Brock. All right.

The Chairman. Any discussion?

Senator Jackson. I second the motion--

The Chairman. You can't move and second.

Senator Jackson. It is all a matter of form.

Senator Roth. Second.

The Chairman. All in favor say aye.

Are there any amendments to Title V?

Senator Roth. Are we beyond Title I?

The Chairman. I mean Title I.

Senator Roth. I have two that I want to offer. On page 5, line 2 -- first, the existing language provides that the Commission shall publish annually the U. S. Directory containing the information specified to provide notice under Section 201(c(3) of this Act for each information system subject to the provisions of this Act.

And the language, I would like to add, is "and a list of all statutes which require the collecting of such information by a Federal agency or other organization."

I think it would be helpful information to know whether or not this information is being collated on their own or whether there is some statutory basis. If there is some statutory basis, we may want to reexamine or modify.

Senator Brock. I don't know where you are.

Senator Roth. Page 5, line 2.

Senator Brock. Subparagraph 2?

Senator Roth. Line 2.

The Chairman. You would change that semicolon to a comma and add the words --

Senator Roth. "And a list of all statutes which require

the collecting of such information by a Federal agency or other organizations."

In other words, I would like to have the statutory basis of collecting this information.

The Chairman. Any discussion by the members?

Senator Jackson. Let me ask a question here.

You know, in every bill that we have passed, we have some kind of a reporting provision. I am wondering, I just raised the question how extensive a compendium we are talking about here. I agree they ought to be able to identify the basis of their publication. That is your point?

Senator Roth. That is my point.

Senator Jackson. I have no objection. Is there going to be a compact that that is going to be so onerous and long -- why don't we try it? It will surely stir them up.

Senator Muskie. That will be implementing the provisions found on page 12, lines 17 to 22, "the Commission shall—(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study," and so on, so I think that the information should be in hand.

Senator Roth. On the point raised by Senator Jackson, we don't want to make a lot of unnecessary reporting requirements; it seems the language should be changed or the report comment on it, in subsequent years they only report additions and

changes. They don't have to go back every year and put in the same material.

Senator Jackson. We will get a reaction on it. See what the reaction is the other way. I didn't intend to object. Virtually, all of the laws that have been passed in recent years have a requirement so we are talking about almost every provision of the Code.

Senator Roth. I think it is a valid point.

The Chairman. If there is no objection, the amendment proposed by the Senator from Delaware will be adopted.

Senator Roth. I would also like to add a paragraph (c) to this Section 103 to provide that the Commission shall -- "Determine whether specific categories of information should be prohibited by statute to be collected by the Federal, State, regional, local government and private organizations because such collections would violate the rights of privacies of individuals."

I think in a sense, Senator Muskie might make the same comment here that he made with respect to my earlier amendment. It is implementing something that we were saying later on. I do feel very strongly that the Congress at some future time and this Commission in its study should concern itself with what data should be collected, and it may be that there should be some statutory limitation on those rights, and that is the purpose of this language.

The Chairman. State it again.

Senator Roth. New subsection (e). It would be on page 7. "Determine whether specific categories of information should be prohibited by statute to be collected by the Federal, State, regional, local government and private organizations because such collections would violate the rights of privacies of individuals."

The Chairman. I wonder if it will all go to the local and State government or whether we ought to restrict it to the Federal Government?

Also we would virtually eliminate the private sector except where somebody is counteracting a Federal agency.

Senator Roth. I am most concerned about the Federal Government.

Senator Jackson. Why don't you confine it to the Federal.

Senator Roth. I will accept that further change.

Senator Muskie. I am aware why this is cut down. I don't

have the basis of hearings and testimony to justify going beyond that. As I understood the Senator's amendment, it is designed to get at that problem.

Senator Roth. Yes.

Senator Muskie. And to encourage the notion that we continue to look at these other areas and be prepared to act when we have the necessary information and recommendations to act upon.

I have no objection to limiting this amendment here, but I wonder if you couldn't have in the report --

The Chairman. You have a provision in the bill that they would report?

Senator Muskie. We could stand on the report to indicate that is what we have in mind.

Senator Roth. Yes.

The Chairman. You confine it to the Federal Government, you modified it. Any objection to that? If not, the amendment is approved.

Senator Roth. With the understanding that the report would expand a little on the further provisions.

Senator Muskie. Specifically point to the fact that we didn't get into the other areas because we do not have an adequate base, but that does not mean that we ought not to be looking into these areas as we gain experience under this legislation.

The Chairman. Are there any further amendments to Title I? If not, I would suggest that someone move that we approve Title I, subject to the right of the SEC --

Senator Brock. Those amendments will be here shortly. I so move.

Senator Jackson. I second the motion.

The Chairman. All in favor of the motion, let it be known by saying aye.

Very well.

Title II starts on page 13, the Bureau is asking for exemption of records collected or funded and used solely for statistical purposes under Section 1, Title 18 of the U. S. Code.

They don't want to have right of access to records they collect solely for statistical purposes. It seems to me that is a reasonable exemption, so I would propose it.

Is there any objection to the Bureau's amendment?

If not, without objection, that amendment will be included. The staff will work it out.

Any other amendments to Title II?

Senator Jackson. Mr. Chairman, there is a question I want to raise and ask Mr. Casad from the investigative staff to comment on it if he won't mind.

On the use of social security numbers, I am not suggesting anything, but there is a real problem here regarding cost; even

though the military, of course, requires the submission of a social security amendment, it is a problem that we ought to know about. I did want to address the issue.

Is it all right to have Mr. Casad who has been involved extensively in investigative work more than I to address the issue?

Mr. Casad. I don't agree with it. You covered it pretty well. That in essence is the problem.

The Chairman. How would it work?

Mr. Casad. The language connotes that the social security number could not be used in many legitimate areas; for example, military services, presently used the social security number as a military identification number. The cost involved in changing the system, it would seem to me to be substantial. Perhaps we should take a look at this and examine it.

Senator Chiles. I agree with that 100 percent. I am thinking about other things,for example, identification, where you are talking about whether it be for food stamps or other things, where you are trying to determine if people are using false identities -- where you couldn't use a social security number. You would be working to promote a lot of fraud.

Senator Jackson. When the banks report your interest, you have to give your social security number; as I read this, you would be prohibited from asking for the social security number and IRS uses this as a means of account identification.

63-619 O - 76 - 5

All these systems would have to be done over. All the costs Mr. Casad estimates run into millions.

We all ought to know. We ought to find out precisely what that impact would be. It is in the form of a question.

Senator Brock. I personally don't see what it adds to the bill to have this particular section, and I would add further that we in the government have insisted and required banks to take social security numbers because what we do, we use that as our base code number with which we relate State income taxes, social security taxes and Federal income tax in order to be sure that people aren't paying one and not another, and it is the Central Recording System. It is the address of an individual, if you will.

Senator Roth. Mr. Chairman, I have had some of the same concerns expressed to me by the University of Delaware, that it would tremendously complicate and increase expenses with them. I recognize the problems of privacy involved here, but I wonder if we might not be wise to give this as an area of study to the Commission itself as a way out rather than to attempt to resolve it quickly. It has very extensive ramifications.

Senator Jackson. Would the Senator yield?

Senator Roth. Yes.

Senator Jackson. I would move to strike this and put it in a study section. I think it would be appropriate.

The Chairman. It is in there. It says study the use of

license plate numbers, social security and universal forms of identification.

Senator Roth. Why don't we just strike it from the section?

Senator Muskie. Could we get from somebody, the staff or otherwise, the justification for the provision? We have heard the negatives which are very persuasive. There must have been a reason why this was included and I am not entirely up on that.

Senator Chiles. Everything was included to start with.

Senator Nunn. The size of the whole world.

Senator Muskie. If you have a universal identification, it would take very little to make personal files available to the central computer. It may seem like a vague kind of fear, but I would like to know more about it. A case for it must have been made. I want to know more before I vote.

The Chairman. We have had a number of hearings on the question of privacy and the argument of people is that if everybody is going to be reduced to a number, the average citizen is going to wind up so his number will be zero. That is the main argument.

Senator Brock. I have the same fear, but I honestly question whether we ought to put in the bill a flat prohibition. It seems to me that a study is warranted. There are certain dangers implicit in it. We ought to prohibit it until we have

had the benefit of a full study.

The Chairman. The objection is if you put everybody in a computer, every computer, somebody could get ahold of everything in a computer. It has been moved to strike this.

Senator Roth. Strike this.

The Chairman. Any further discussion?

Senator Roth. Question.

Senator Muskie. As I understand it, and I want to be sure it is before us, you have got one linkage number of that kind, you can use it to convert all of the data banks and all the information files in the Federal Government to one giant data bank making any piece of information relating to any individual in any file respond to that one number.

Now, I am not sure that we examined closely enough some of the ways of strengthening these provisions to avoid the horrors that some members have already suggested. Before we jump too strongly to that side, I just raise the point because I feel a little uncertain about my own knowledge in this field.

Senator Roth. I very frankly have some of the same concern which is expressed by Congressmen Rosenthal and Goldwater when they came to our side and testified. They raised a very legitimate problem. I don't feel that we have the opportunity to study the problem in sufficient depth to make the definitive decision now and, for that reason, the Commission is appropriate.

One of my concerns is if you do away with this, you will

probably just have some alternative so that will accomplish the same thing. We are better off making a more carefully, precise study to see if we will come up with the solution.

Senator Jackson. I share Senator Muskie's concern. With the only thing we are sure of, we are confronted with immediately. I hope they will study it and see if they can't come up with an alternative. We are confronted immediately with a heavy expenditure of funds in connection with the current investment of IRS alone -- the information that is fed in on all savings accounts, would have to be completely undone. Corporate dividends -- it covers the whole area using the social security numbers, and my suggestion would be that we have some language, Mr. Chairman, in the report here that we have struck this because of certain investments already made, we are just talking, Chuck, about the use of social security numbers.

Senator Percy. I would like to comment on this.

Senator Jackson. We are concerned with the danger of this sort of system being institutionalized to the point where it can all be fed into one central system in which there could be a misuse of that information and I share that. The only problem that we face immediately is not having the facts here, but we do know that it runs into the millions to completely change the reporting system right away, but why don't we have some language, expressing, Mr. Chairman, the reasons for this and our fear of the direction we are going by utilizing on a

universal basis, the social security number approach. I think that is Senator Muskie's same concern.

Senator Percy. Mr. Chairman, I am sorry I was late, but I can say the cloture vote before the final, last cloture vote on the agency of consumer advocacy is set for the 18th following the recess.

I would like to speak on this item because it was the one that I originally had the same --

The Chairman. I enjoin upon you not to give anyone else such a mess of political potage as you did some of the farmers.

Senator Percy. I was somewhat concerned about the same section for the reason that you interrupt procedures already established. I met with Congressman Goldwater. This provision is in the House bill. I note very, very strong feelings the House has about it. It is their contention and I am now convinced if anyone wants to really put together a system that would put everyone on a numerical basis and put everything together as one common number, the social security number is the key to the way to do it. The more we get in it, the more troublesome it can be.

I would be compelled to vote against the amendment. I can assure my colleagues, that at least Congressman Goldwater, who is on the committee for the House bill, is very strong about it.

Senator Chiles. If that is the danger, you have to see

that maybe the number doesn't get combined, but to strike the use of the number as being able to use that as an identifying thing, it seems like to me it will cost untold dollars, untold dollars, and it seems like to me we are just going the reverse way -- to say we don't want a number is like saying we are not going to allow people to have middle initials because there is a danger here.

I see the danger. Maybe you want to speak to it in this bill that you will not allow the combination -- some way of putting together any machine that starts to group this, but for identification, what is IRS going to do about dividend identification?

We are beginning to use the number sum to prevent fraud. It seems like to me if you are not going to be able to use it in cross-checking or preventing fraud, then privacy is one thing, and I am for that, but I couldn't be for this bill if I thought we were going to knock all that out.

Senator Percy. As I understand, it will not change IRS at all because that exists as a matter of law right now. You do not change any existing laws.

Senator Brock. But the problem is IRS gets its information from States, banks, S&L's; any lending and depository institution as of now under the law requires the social security number to be filed with the name, the purpose of which is to have a central address code for each individual by which they furnish

information to IRS so they can cross-check against fraud or against internal revenue abuse, not reporting dividends, not reporting interest earned, and that sort of thing.

Further, we are on the brink of going to an electronic funds transfer system in this country. It will save an awful lot of money in terms of our business dealings for the consumer to prohibit the application of the one device by which you use that system is, I think, insane. It is penny wise and pound foolish.

The Chairman. I am informed that the provision has been deleted from the House bill.

Senator Jackson. The social security?

Senator Brock. Yes.

The Chairman. A comparable prohibition. A prohibition on the use of social security.

Senator Chiles. They have deleted it?

Senator Brock. They ran into the same problems we did.

Senator Jackson. Let me ask one question.

We are all, I think, in general agreement on the danger that is inherent in the use of numbers because you are going to have to use numbers one way or the other. The danger is pulling them together and centralizing them and putting them in one bank.

Senator Brock. Yes.

Senator Jackson. How much would it cost to carry out this

section? Surely we can get an estimate on that. The whole reporting system on interest on loans, savings accounts, dividend reporting -- all of it is predicated on this, all of the military reporting is based on -- and that would be prohibited on your social security.

Senator Percy. The key phrase is "required by Federal law." All the banks are required by Federal law. There is no attempt to prevent them from furnishing what they are now. What you would so is someone arbitrarily deciding they are not going to cash a check or will not issue some form of credit unless you give them your social security number.

Senator Chiles. You will have to change all the Senate I.D. cards because they have the social security number.

Senator Jackson. Let me ask you the question; I don't know the answer. I am not sure just what is required specifically by Federal law. I don't think on the military side that that is specifically required that they use social security numbers. They are doing it because it takes care of the dependents and so on. If you have your physical, you know they ask you for your social security. So I don't know, Senator Percy, what areas are specifically required by Federal law.

I will withdraw the motion. I would just like to know what this is going to cost because without that knowledge, I think we are --

Senator Brock. I don't think you can give a cost answer to a question that is still in flux. The thing that frightens me even more, what I consider an excusable cost on the economy is what the future cost would be because we are very much moving toward a more simplified recordation system and this is the part and parcel of it.

What you are trying to do is deal with the central data bank, with the potential abuse of privacy. I don't see that you can abolish drowning by milk by outlawing milk. That is what you are trying to do by outlawing the social security number. I think it is wrong.

Senator Roth. I don't know who made the motion; if the distinguished Senator from Washington withdraws it, I would make it again.

We have inadequate knowledge to make a definitive decision at the current time.

Number one, we don't know exactly what the law does require.

SEcondly, you do have a problem. What will it cost the Federal Government and other agencies? I would like to point out again in view of what was written by the University of Delaware, this will have tremendous cost to the private sector as well, and I think, third, Lawton Chiles raises a very important point, this is being used to eliminate fraud in some of our programs. Perhaps it is not essential, but I don't see how we can make that decision now. I strongly urge, particularly

since the House has receded on it, that we move in the direction to have a study.

Senator Percy. We are not sure about the House situation. I would like that clarified. The markup isn't until tomorrow morning at 10 o'clock.

I am advised it is not in that bill.

Senator Nunn. Can we call the question on the bill?

Senator Brock. I don't care what the House has done. Our action is independent.

Senator Muskie. I have no desire to delay it. The debate on this provision highlights the issue involved in this entire bill. There are benefits to the computer age. Apparently it is like blowing into a gale. The benefits are so obvious and so easily stated that we are willing to give up our privacy in order to get them.

If you get this close, that one number can make the private lives of each of us subject to anybody's finger on the button--we would weigh the benefits. The rest of this seems to be peripheral.

I am not expert in computerizing, but it seems to me that the key to the computerized society is the day we arrive at one number that can tie us all together. That is what this is. The rest is peripheral.

I suspect we don't know enough about it to take this leap. I don't really object to that. We ought to focus on the fact

that the rest of it is rather unimportant. It is a real attack on a threat to privacy, if we are willing, and the momentum seems strong to accept the social security number and all its implications of spreading our private lives throughout our society.

Senator Roth. None of us have any judgment on the other side. You raise a very pertinent case. We feel it needs further study than has been made at the present time.

The other point I would like to make is that it is my understanding that the rest of the bill is to prevent from happening what you have foreseen. The whole purpose of this legislation is to protect privacy in some single method of being used. It can't be said that we are doing nothing if we just make a study.

The rest of the bill is to prevent the development of another number that has the same result.

Senator Chiles. No, it is more than that.

Senator Brock. It is more.

Senator Chiles. It is to prevent a combination of interlocking data building up and coming together.

Senator Brock. Yes.

Senator Muskie. The key to combinging them is something so simple as a social security number.

Senator Brock. In working with computers, any system can be devised for setting an address mechanism to find any

individual, however you want to do it. You can take the first two letters of the last name and last three letters of the first name and the street numbers.

Senator Muskie. There is no consensus about any key as there is about social security.

Senator Brock. If you strike social security numbers, you don't deal with the problem which is the central bank at all. The rest of the bill deals very forcefully with disclosure, with access, and all the other things that are important in privacy.

I don't think striking "social security" has anything to do with the basic thrust of the bill.

Senator Muskie. The point I am making is not directly related to the mechanis in that sense. The point I am getting at is that there are such obvious temptations that come from combining the information about the 200 million of us that are members of this society.

When we get to the threshold of the benefits, we are willing to surrender the benefits whether it is by way of security number or something else.

Senator Brock. I am going to stay right here. I am just going to answer the phone.

Senator Jackson. Can we take this up out of order? This is a matter pending when Senator Percy was here. If we could take up our resolution for the Permanent Subcommittee on

Investigations, this would be a request that we worked out jointly of $86,000, Chuck, which we will modify. Senator Percy has indicated a need -- it is $85,000 instead of $86,000.

The Chairman. We voted not to exceed five minutes?

Senator Jackson. It won't take that long. We ask that the resolution before you be revised to reflect that total figure of $85,000 instead of the $86,000 and that it be modified accordingly.

The Chairman. Is there any discussion?

Senator Jackson. We will modify our letter to you.

The Chairman. All in favor of reporting the bill for more money for the Permanent Subcommittee, hold up your right hand.

Let the record show unanimous approval.

Senator Jackson. I am wondering if we can't, and I won't change my mind on the floor, I think we are all in agreement on the idea that we want to avoid, and this is part of the problem, we want to avoid a situation of a number -- if it isn't the social security number, it could be something else. We have national health programs coming up. You have the number business again. We will start a whole series of numbers. This is going to be, whether we like it or not, a major problem. Rather than having a lot of numbers floating around, the tendency now is to identify with just the singular social security number.

I think secondly the general consensus, if I read our

comments here correctly by our colleagues is that what we want to avoid is the pulling together of all of this in such a way in which it can be used to interfere with the civil liberties of our people.

No one feels any stronger about it than any member of the committee. What really bugs me is if it should go out just the way it is, I just don't know how much it is going to cost. The military is not covered by this, by the way. That is done by, staff checked it, that is done by simple Executive Order, and in the interest of savings to the government, so my recommendation would be that we put language in the report to explain properly our deep concern about the growing use of the social security numbers and reiterate the study that ought to be given top priority on the use of social security numbers in a manner and fashion which could interfere with the civil liberities of our people.

Senator Chiles. I would hope if we put it in, put where the number is being combined. It is a legitimate thing to acquire some identification for someone who is applying for some kind of a government program, whether it be a crop allowance or whether it be an emergency disaster relief or food stamps or something else.

One reason people fall out with these programs so bad is where there is fraud in them, where people are applying more than one time, and where they are getting money improperly --

to me it is a perfectly legitimate use of social security or any tool we can come up with to try to prevent fraud.

Senator Jackson. That is the balance you have to deal with constantly.

Senator Chiles. The danger is in the combination as Senator Muskie has pointed out.

We are dealing with a bill right now that doesn't contain anything about the private banks because we have decided that we can't handle that now, and we are going to study it. When we get into privacy, that is important, I think, some of the abuses that are in the private banks, are more than anything we are dealing with in this bill. And if we allow that, we could certainly allow the study on the possible dangers of social security.

The Chairman. Could we vote on this?

All in favor of deleting Section 205 and renumbering appropriately the subsequent sections?

Senator Jackson. With appropriate language in the report to explain it.

The Chairman. Yes.

All opposed, raise your right hand. 8 to 1.

The committee will put in the report appropriate language.

Any further amendment to this?

Senator Nunn. I have got one quick question I might point out. On page 14, this gets into the same argument -- if you

look at No. 2, this is saying each Federal agency should collect information to the greatest extent possible directly from the subject individual when the information may result in an adverse determination about an individual's rights and so forth.

That sounds real good, but let me explain what we will run into.

The Chairman. Give me the page number.

Senator Brock. Page 14, subparagraph 2.

The Chairman. I see.

Senator Nunn. Senator McIntyre and I, he has taken the lea we have been hearing about duplication, great duplication.

Small businessmen are about to go crazy because of the form and paper work. The average radio station has to provide several pounds of forms. It takes two or three years for them to read through it to get any decision. We are going contrary to the Federal Reports Act. We are telling them the opposite of what we were trying to do. Trying to get together and not require the same man to fill out the same form, so I am not going to offer an amendment.

The only way I know how to change it is delete it altogether or substitute the word "practical" for possible, but I do caution, and I think everybody ought to realize the direction we are going in in this particular language here.

We are saying to the Federal agency, "Boys turn loose those

Federal forms." We want more of it. Put it really on the small businessmen of this country. That is what we are telling them. That way OMB couldn't say to two agencies, "You have the same information coming from different sources, combine the forms." I really don't know quite how to handle it.

The Chairman. This is restricted, however, to information where it may result in an adverse determination against a person.

Senator Nunn. Any form you might fill out could result in an adverse determination against an individual. I don't know any agency that has any form -- perhaps only the Census agency and you are subject to criminal provision with that. Any form you fill out subjects you to an adverse determination if it goes to the Federal bureaucracy.

Senator Jackson. Especially if it gets on the computer.

The Chairman. On what line is the specific amendment?

Senator Nunn. I don't have one. I don't know how to mend it. I don't want to strike it. The only way to successfully mend and to keep it from being completely contradictory to what we are working on in other areas is to strike it. You could strike the word "possible" and put in "practical" and some words that say "subject to the intent of the Federal courts."

It is on line 3, page 14. It is directly contrary to the intent of Congress in a lot of other respects.

Senator Muskie. As I read that language, it is designed

to insure that any file on a person shall to the fullest extent possible be based on information derived from him rather than from other sources.

Senator Nunn. Other sources are other Federal agencies. That is the way I read it. I gathered this is designed to get them away from hearsay and down to information that the individual himself has had a chance to verify. That is how I read that language.

Senator Jackson. It places the burden, as I understand it, on the Federal agency to go to the individual and avoid the hearsay.

Senator Brock. May I suggest a compromise. Why don't you explicitly spell that out and we say by no definition are we trying to further burden the businessmen with further required reports. This is to be within the context of the Federal Reports Act.

If you say that you are covered.

Senator Jackson. Those are the magic words.

Senator Nunn. That would help it.

The Chairman. Priscilla Alden said, "Speak for yourself, John." This is information from the individual. It gives the individual the opportunity to present the information in the best light as they can for themselves.

Senator Brock. If you would modify the report to include that.

The Chairman. Yes.

Senator Nunn. Scratch the word "directly". It wouldn't come directly from the individual to the agency in question, but it would still hve come from the individual.

Senator Brock. The basic originating agency would be covered.

Senator Muskie. How does eliminating the word "directly" help?

The Chairman. This protects the individual and allows them to speak for themselves.

Senator Muskie. It says, "when the information may result in adverse determinations about an individual's rights," and so forth, the information ought to come from him.

Senator Nunn. Yes, I agree with you, but not 10 different times.

Senator Brock. If you apply the basic statute to one agency that gets the original information, then that information, if it complies with the law, should -- you shouldn't have to get the individual to file another report that says exactly the same thing to a different agency.

He is trying to leave out repetition.

Senator Jackson. Let us get report language.

The Chairman. Yes. I agree with you, "practical" instead of "possible".

Senator Nunn. I would offer that as an amendment,

"practical" instead of "possible".

The Chairman. If there is no objection, we will change "possible" to "practical" on line 3.

Senator Brock. May we submit report language to Sam Nunn to see if it is adequate?

The Chairman. Yes.

Senator Nunn. I have another amendment on page 23, section (g), which is on line 3, page 23.

"(g) Each Federal agency covered by this Act which maintains an information system or file shall assure that no personal information about an individual is made available from the system or file in response to a demand for information made by means of compulsory legal process unless reasonable efforts have been made to serve advance notice on the individual."

What I would submit, Mr. Chairman, is what we are saying there, we are telling the agency to defy the legal process if they determine that reasonable efforts have not been made to give advance notice.

I don't think that is what we mean. We would be placing the agency or whoever is doing it between obeying the court order and obeying this law. I would like to see us change it that "Each Federal agency covered by this Act which maintains an information system on file, make reasonable efforts to serve advance notice on the individual when the file is made available under compulsory legal process."

It is another way of saying the same thing without plaguing the agency, without defying this law or the compulsory legal process.

Senator Jackson. I see nothing wrong with it.

The Chairman. That seems to be an improvement. We will take your longhand sheet.

Senator Jackson. I second the motion.

The Chairman. Any discussion? All in favor of the amendment, raise your right hand.

Very well.

Any other amendments to Title II?

No further amendments to Title II, the Chair will take a motion that it be approved subject to the previous understanding by any members about the SEC.

Senator Jackson. I so move.

Senator Brock. Second.

The Chairman. All in favor of approving Title II, under those circumstances, raise your right hand. Very well.

Senator Nunn. Title II, I am in favor of it and I voted for it, but this language on page 26, lines 19 and 20, I believe that is in Title II. Perhaps this would have to be a judicial determination, but if you look at line 19 or 20, we are talking about an exemption for investigative information, and we have an exemption here which specifies where such information has been maintained for a period longer than is necessary to

commence criminal prosecution. I don't know what "longer than necessary to commence criminal prosecution means."

I will ask the staff to look at that. Maybe that is as close as we can come to properly defining it.

The Chairman. I might state that I am informed it is identical to the language in the Freedom of Information Act that we since passed and I understand is about to be signed into the law.

Senator Nunn. If we know what it means, that is fine.

The Chairman. It is sort of left up to the agency to determine.

Senator Brock. The agency or the court?

Senator Jackson. Mr. Casad went into this. He was satisfied. What was your comment?

Mr. Casad. We had the same concern, Senator Nunn, that you just enunciated. In Print 5 we reviewed it again thoroughly. We were satisfied that there would be no problem.

Senator Nunn. I will accept that. I got behind on Title II, but on the mailing list, this is a sort of considerable amount of frustration with people throughout the country. On Section 207, page 29 -- Section 207, lines 12 and 13: "An individual's name and address may not be sold or rented by a Federal agency for a commercial purpose."

Do we really intend to make that just a commercial purpose or any purpose? For instance, could --

The Chairman. I think it could take care of themselves. Federal agents say they can't afford to give them out free.

Senator Chiles. You could sell them for other than a commercial purpose.

Senator Nunn. You could sell it to a political candidate. Do we intend that?

Senator Brock. I haven't thought about that.

Senator Jackson. That is an unprinted amendment.

Senator Nunn. It may be construed as a commercial purpose.

Senator Brock. It may be.

Senator Chiles. It is bad business.

Senator Nunn. I don't think we intend for any of these Federal lists to be sold.

Senator Brock. And direct mail solicitation for Korean Orphans?

Senator Nunn. Charitable institutions. I just pose the question. Don't we intend to bar the selling of Federal mailing lists?

The Chairman. That is what I think ought to be done.

Senator Nunn. If you struck commercial and put the word "any" in there -- there may be something wrong in that. Shall not be sold or rented, period.

Senator Chiles. Strike "for a commercial purpose, shall not be sold unless."

Senator Brock. Strike the words "commercial purposes"

down in the body under 3 also.

Senator Nunn. I agree, it ought to be struck all the way through there.

The Chairman. I would strike out the words as Senator Brock suggested, "for commercial purposes," and that will accomplish what is desirable.

Senator Brock. We ought to strike the words "commercial purposes" and "commercial" in 1 and "for commercial purposes" in 3 -- all the way through.

If you are going to do it, you ought to be consistent.

The Chairman. Where else?

Senator Brock. All on line 2, strike "for a commercial purpose".

Under 1, you repeat those words, they should be stricken, shouldn't they?

Senator Chiles. The others are the exceptions. If you are dealing with the -- if you said they can't sell them, there is no reason to strike them.

Senator Nunn. I think it ought to be stricken to be consistent.

Senator Muskie. A period after agency?

Senator Jackson. Let me ask, I understand from staff there is a problem here, I just raise this question again -- the blind group and the Indians have asked -- they do buy these lists not for commercial purposes, but for appropriate

nonprofit purposes. What happens?

They will not be able to buy it. As I understand it, it is important in connection with what they do. I don't know who else is affected.

Senator Nunn. You are talking about charitable institutions. I posed it as a question.

Senator Brock. If you let one group have it for a non-commercial purpose, they can in turn sell it to anybody in the country, so what have you gained? You either ought to do it or not, I think.

Senator Roth. I would like to raise a slightly different question while we are on this. Does section (2) permit the head of an agency to use names and addresses for lobbying purposes for its agency functions? In other words, can they make these names available to promote, say, appropriations for their agency? It is subsection (2). It says, "the head of the agency has certified that the commercial use of such names and addresses will aid in the performance of the agency's functions."

Are we authorizing the head of an agency to use such names and addresses to promote its own programs or appropriations? I question the wisdom of that.

The Chairman. We have a statute designed to prevent any agency of the Federal Government to spend any part of its appropriations for lobbying purposes.

Senator Roth. It might be worthwhile mentioning in the report that this new language is not revoking the old. That could be a very valuable aid to the lobbying effort. I am suggesting that we make it clear in the report that we are not authorizing the use of names for lobbying.

Senator Jackson. They are now selling them, Interior Department to the Indians?

Do I understand the amendment to be that on line 12, it would simply read "An individual's name and address may not be sold or rented by a Federal agency," period, and all the rest would be stricken?

The Chairman. I don't know whether we have a consensus about this.

Senator Roth. He made a motion that we strike "for a commercial purpose" wherever it appears, per se.

I second that.

Senator Muskie. The effect is to prohibit sale. Put the period after "agency" on line 13 and delete the rest?

Senator Jackson. Yes.

Senator Brock. You have some exceptions which are obvious If the sale or rental is obvious by law, it may be something we ought to keep.

Senator Muskie. Unless it is authorized by law.

The Chairman. I would suggest that maybe the best way to do this would be to insert "An individual's name and address

may not be sold or rented by a Federal agency unless such action is specifically authorized by law," and strike the rest.

Senator Jackson. I move the amendment to the amendment or the amendment as modified.

Senator Brock. You are not striking the last sentence?

The Chairman. In other words, strike out the whole section and then reword it like this, "An individual's name and address may not be sold or rented by a Federal agency unless such action is specifically authorized by statutes or as provided by law."

Senator Brock. I think you want to keep the last sentence in the paragraph "shall not be construed to require the confidentiality of names and addresses otherwise permitted to be made public." Strike everything above that and substitute your language.

The Chairman. Any objection?

Senator Jackson. You would knock out (b), too. There is no point to (b).

The Chairman. I am going to write a whole lot of letters when I get home. I am on every sucker list in the United States.

Senator Chiles. Mr. Chairman, my colleagues have found another glaring error and they have asked me to be sure to raise it. On page 12, subsection (2), where he is talking about "The Commission shall include in its examination" --

The Chairman. Will you wait, Senator Jackson?

Senator Chiles. They name a number of things that the Commission shall include in its information activities or its examination, and they name hotel, travel, entertainment, restaurants and then they say, "The Commission may study such other information activities necessary to carry out the congressional policy embodied in this Act." That ought to end with a period. While they add "except that the Commission shall not investigate information systems maintained by religious, charitable, or political organizations."

Why are we exempting religious, charitable or political organizations if you are talking about carrying out the policies of the Act as to privacy?

The Chairman. That has been one of the great complaints about the use of computers to select information on these subjects.

Senator Brock. That is what we ought to be worried about. That would justify some study to prevent abuse. We are not going to add it up to say that they have to study it. To they can't -- it looks like to me it is a pretty glaring thing.

The Chairman. You have got your doctrine of the separation of church and state --

Senator Brock. I didn't know that we separate politics from the state.

The Chairman. I think it is a pretty good thing to do. The Subcommittee on Constitutional Rights conducted a study on use of the Army, military intelligence, to spy on situation violence, and the favorite information they collected on people was their political views and membership in political organizations --

Senator Brock. This is a bill to safeguard and not to abuse.

The Chairman. This says this is grass the Commission can't travel on.

Senator Chiles. Then a religious organization or political organization can invade my privacy any time they want to or a charitable organization.

The Chairman. This is keeping you from invading theirs.

Senator Brock. It depends on who is trampling on whom.

The Chairman. This keeps the Commission from going into the field of investigating what kind of information churches, charitable and political organizations have.

Senator Nunn. You are saying the Rockefeller Foundation could keep a computer in New York and have every single being in the world charted down there, and this Commission couldn't even look at it?

The Chairman. What interest would the government have?

Senator Nunn. Or the Ford Foundation.

The Chairman. I think this is a very good provision.

I don't think a governmental commission ought to investigate what kind of information religious organizations are collecting or charitable organizations.

Senator Chiles. What is to prevent a restaurant association from setting up a nonprofit organization that is going to be their computer bank or their information system?

The Chairman. This doesn't say nonprofit.

Senator Chiles. It could be charitable.

The Chairman. Or not. A restaurant is a commercial business.

Senator Brock. Mr. Chairman, you and I both know how many times we have seen abuses of charities in the last 20 years, abuses of tax exempt foundations by individuals for a political purpose.

I don't see how you can exempt this sort of thing. How do you define the word "religious" or "charitable" or "political", but it looks like a carte blanche.

The Chairman. No, they can't. If it is a jimsonweed, you can't call it a rose and get away with it.

Senator Brock. It has been done before.

Senator Jackson. It looks to me that we have given the Commission plenty to do. They can postpone getting into this one.

Senator Chiles. I don't think we should give this to them. It bothers me that you say they can't. You say the Commission

may study such other information activities necessary to carry out the congressional policy embodied in this Act, but even if it was necessary to carry out the congressional policy embodied in this Act which we are saying is important, they can't do it if it is religious, charitable or political. You have excepted it.

The Chairman. The First Amendment says the same thing.

Senator Percy. Can't we cover that in the report?

The Chairman. I don't see how in the First Amendment you can put a provision to establish a commission to investigate what kind of religious organizationsor also about political organizations.

Senator Brock. How about the First Amendment as it applies to medical records?

The Chairman. The First Amendment --

Senator Brock. Doesn't apply to people who are sick.

Senator Nunn. Could we eliminate everything but religious? Anything is a charitable organization. All you have to do is just qualify with the State government. This could be the greatest loophole in the law.

Senator Brock. I am charitable, I am not operating for profit.

Senator Chiles. I am not sure about the Commission going into a 3-2 split on parties.

Senator Brock. If the First Amendment protects just

against religious incursions, then we don't need to restate it. So strike the exception.

The Chairman. It is a good idea to make it certain. There might be a commission that doesn't care much about First Amendments.

Senator Brock. I doubt if the courts would go along.

Senator Nunn. We are invading the privacy of everybody else here.

Senator Brock. Either you are or you are not.

Senator Jackson. Why don't we confine the prohibition to religious organizations or institutions?

Senator Nunn. I second that.

The Chairman. I think the same thing about political. You should have seen what the Army collected on the political views and organizations.

Senator Brock. But this whole bill is designed to stop that, Mr. Chairman.

The Chairman. Then why make a study?

Senator Brock. The Army is not involved.

The Chairman. The most outrageous collection of information that I have ever seen was by the Army Intelligence. Even when a Member of the Senate went to Greensboro, North Carolina, that garden of Eden, and the military intelligence put it in the report to Army Intelligence what the Senator said in his speech.

Senator Brock. What does the Army have to do with a

political organization?

The Chairman. A lot in '67 and '68. They had those people spying on the protestors on political things.

Senator Brock. That has nothing to do with that amendment.

Senator Chiles. Then you would put the U. S. Army in here?

The Chairman. Oh, no. They had the U. S. Army spying on the people to determine what their political beliefs were, and we just say the Commission is not going to study how to spy on people about their political beliefs.

Senator Brock. You are saying they can't stop it. You are prohibiting any study?

Senator Nunn. Then we ought to eliminate all of them.

The Chairman. The Commission may study such information activities necessary to carry out the congressional policy embodied in the Act except that the Commission shall not invest in information systems maintained by religioius, charitable or political associations.

Senator Brock. I move that we strike "charitable or political".

Senator Nunn. Second.

The Chairman. You want a study made by the government how to computerize --

Senator Brock. I thought this Commission was to try to

stop it.

Senator Muskie. It seems to me there ought to be a way to accomplish both of these. What the language of the bill is intended to protect is to protect information that which is in the files of these kinds of organizations from those seeking it for improper purposes and what these gentlemen are concerned with, these Senators, it also protects these kinds of organizations who themselves are engaged in improper activities impinging upon privacy. Both objectives could be served by appropriate language.

Senator Percy. Mr. Chairman, I think what we are trying to prevent is mischievous activity, and I would offer this substitute amendment that would keep the language as is, but following the word "organizations," comma, "unless it makes a formal determination and so notifies Congress that such investigation is essential in the performance of its functions."

Senator Nunn. If you have an organization like CREEP or anything else, you are saying in spite of this effort toward privacy, CREEP can sit with a massive computer center on everybody and have every single detail and this is taboo. They can go into the First National Bank in Perry, Georgia, and get all that information by subpoena, but they can't find out anything about what CREEP is doing to the privacy of the individuals in this country.

It is incredible. I understand the chairman's argument

about religious organizations. To say that political organizations are exempt and have the committee studying every private business in this country to me would be incredible.

The Chairman. I wish you had sat with me on the Army Surveillance hearings.

Senator Nunn. I don't see the point.

Senator Brock. It has nothing to do with this comment.

The Chairman. It has everything. It says this Commission shall not investigate the political files of political organizations.

Senator Brock. That is right. So the Commission couldn't stop, the Commission you referred to. The Commission can't even deal with it.

The Chairman. This stops the Commission from studying it.

Senator Brock. It sure does, which means the abuse is going on.

Senator Nunn. I would be more concerned about the travel or hotel industry or the medical industry than I would the political industry.

Senator Brock. There has been more political abuse lately.

Senator Nunn. That is where the abuse is coming from.

The Chairman. It was where they started to invade the intelligence, trying to get it from a political organization.

Senator Brock. You will prohibit them from stopping that.

You exclude them from any coverage at all with this language as written.

The Chairman. No, it keeps them from studying things that are none of the government's business.

Senator Chiles. The business of this bill is privacy of the individual.

The Chairman. That is right. That is where you protect it.

Senator Brock. By saying you can't investigate.

The Chairman. It is to keep the Commission from devising methods in which to take the privacy out.

Senator Brock. If you think that is what the Commission is going to be doing, you better oppose it because you are giving this Commission power to do everything else.

The Chairman. I would oppose, as long as the good Lord gives me the breath of life, any effort on the part of the government to mess in a political or religious organization. There are a lot of fraudulent charities. I am not so much concerned with them.

Senator Jackson. Suppose we put in "bona fide" religious, charitable or political organizations? That might exclude CREEP.

Senator Brock. I hope so.

Senator Chiles. We could add "with benevolent intention."

Senator Jackson. I was trying to protec the two-party

system.

Senator Roth. Do we have a motion?

Senator Brock. Strike "charitable or political".

Senator Chiles. You have made a good point. We are trying to protect individual privacy and yet we are setting up a commission to go in here in every other organization from little banks all the way down the line. That point goes to the whole bill and goes as much to the other organizations as it would to a political organization.

The Chairman. I think this is a protection of privacy.

Senator Nunn. I would agree and I am leaning that way.

The Chairman. If you had as much experience as I, I spent a year and a half investigating the use of military intelligence that was spying on situation violence and computerized information.

The military intelligence in Chicago had a dossier on the political activity of Congressmen and a man who is now a Member of the U. S. Senate.

Senator Percy. I resent it.

Senator Nunn. You said CREEP did the same thing.

The Chairman. No. That caused the trouble. CREEP tried to get intelligence from the Democratic National Headquarters.

Senator Brock. You think this Commission shouldn't have any jurisdiction on that?

The Chairman. If anybody, anybody who has any information

about my political views or affiliations, that is my business, and not the Federal Government's.

Senator Chiles. What about the ones on the other side?

The Chairman. That is Watergate. Let me tell you. You all see -- they had peoples' names over here in the Department of Defense --

Senator Brock. We are familiar and we are opposed to it, we are opposed to the sins of both administrations.

Senator Percy. Let us vote on the Brock amendment and see where we stand.

Senator Nunn. That is to delete the words "charitable" or "political" and leave "religious" like it is.

The Chairman. It has been moved on line 15, page 12, strike out the word "charitable" or "political". All in favor of the motion raise your right hand.

Let the record show the chairman votes against the amendment.

Opposed?

Senator Nunn. I have the proxy of Senators McClellan and Allen. They both wanted to be recorded aye.

Senator Brock. It is carried, I assume?

The Chairman. Yes.

Any further amendments to Title III?

(Discussion off the record.)

The Chairman. Senator Muskie will be back.

(Discussion off the record.)

The Chairman. Section 203(a) here is the only SEC amendment.

Senator Jackson. They have done it to Print 4.

The Chairman. On page 27 they would add a new section (d), subsection (d), "The provision of this Act will modify the information for the purpose of providing disclosure to the public pursuant to the requirements of law administered in the SEC," and so forth.

(The SEC amendment to be furnished follows:)

COMMITTEE INSERT

The Chairman. I think we have adopted this in the technical amendments, "Nothing in this Act shall be construed to permit the withholding of any personal information which is otherwise required"-- to permit the withholding of any personal information.

Senator Percy. Mr. Chairman, so far as I am concerned, the staff indicates they have gone over this and it is already covered.

Senator Jackson. What I think they are confusing is that the SEC has interpreted this bill as one which prohibits the dissemination of information which obviously must be made public in connection with disclosure law.

This bill deals with personal information and not with the whole question of disclosure per se. Isn't that the distinction?

Senator Chiles. Why don't we just adopt it and let it work out in the drafting of it.

The Chairman. I see no great objection.

Senator Percy. I second that.

"Nothing in this Act shall be construed to permit the withholding of any personal information other than that required to be disclosed by law or any regulation thereunder."

We already have that.

Senator Brock. Let us take it and let the staff modify to conform it.

Senator Jackson. Second it.

Senator Huddleston. Can we report 3341?

Senator Brock. Let us report this one.

Senator Jackson. I move that the bill be reported as amended.

Senator Brock. I second.

The Chairman. All in favor of reporting S. 3418, as amended, Confidential Committee Print No. 5, as amended? Let the record show --

Senator Percy. Senator Javits.

Senator Jackson. Also Senator Muskie.

Senator Huddleston. The Per Diem bill, 3341. I want to move that we report it.

Senator Percy. I have one amendment. I offer the following amendment which I discussed with Senator Metcalf and it seemed to have his concurrence. We are providing for per diem for the Executive Branch, for an increase for Senate staff, but we still do not hvae any per diem, travel, but no per diem for Senators' staff when returning on official business to their own home State. The amendment provides no reimbursement within 120 days after any primary or general election in which the Senator is a candidate and the Senator must personally certify that the trip was for official Senate business.

We have, the Senators, duplicate homes. Our staff do not have. When a Washington staff member goes back to the State,

they have no provision, they are the only government employees who have no provision to be compensated for that, so I offer this amendment to 3341.

The Chairman. All in favor of that amendment, let me know.

Senator Huddleston. There is one technical amendment. This is in the folder. It is just a clarifying amendment.

The Chairman. All in favor of adopting a clarifying amendment? All right, it is adopted.

Senator Chiles. Mr. McClellan asked me to offer an amendment as to any increase.

"Provided that any increase in costs of per diem or mileage that results from this legislation during the period prior to July 1, 1975, must be funded either from previous approved appropriations or from budget requests officially before the Congress at the time of the enactment of this legislation."

If you don't, you will have a rash of provisions. We ought to adopt this. We will have to use existing funds, you are not just going to have to raise the budget right now, you will have to work within existing funds. If you don't do this, the Appropriations Committee would have to ask for this anyway.

Senator Percy. Would that come from the contingent fund? I am informed it comes from the consolidated allowance.

Senator Chiles. You are dealing with every agency. It will have a major effect on your appropriations. I am sure the

Appropriations Committee will ask for this bill if they don't get an amendment.

Senator Brock. I second it.

The Chairman. All in favor, say aye. Opposed: All right, it is passed.

Thank you, gentlemen.

(Whereupon, at 5:00 p.m., the committee recessed, to reconvene subject to the call of the chair.)

Calendar No. 1127

93D CONGRESS
2D SESSION

S. 3418

[Report No. 93–1183]

IN THE SENATE OF THE UNITED STATES

MAY 1, 1974

Mr. ERVIN (for himself, Mr. PERCY, Mr. MUSKIE, Mr. RIBICOFF, Mr. JACKSON, Mr. GOLDWATER, and Mr. BAKER) introduced the following bill; which was read twice and referred to the Committee on Government Operations

SEPTEMBER 26, 1974

Reported by Mr. ERVIN, with amendments

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State and local governments, and other organizations regarding such information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

~~TITLE I—FEDERAL PRIVACY BOARD~~

~~ESTABLISHMENT OF BOARD~~

~~SEC. 101. (a) There is established in the executive branch of the Government the Federal Privacy Board which shall be composed of five members who shall be appointed by the President by and with the advice and consent of the~~

Senate from among members of the public at large who are not officers or employees of the United States. Not more than three of the members of the Board shall be adherents of the same political party.

(b) The Chairman of the Board shall be elected by the members of the Board every two years.

(c) Each member of the Board shall be compensated at the rate provided for GS–18 under section 5332 of title 5 of the United States Code.

(d) Members of the Board shall be appointed for a term of three years. No member may serve more than two terms.

(e) Vacancies in the membership of the Board shall be filled in the same manner in which the original appointment was made.

(f) Vacancies in the membership of the Board, as long as there are three members in office, shall not impair the power of the Board to execute the functions of the Board. Three members of the Board shall constitute a quorum for the transaction of business.

(g) Members of the Board shall not engage in any other employment during their tenure as members of the Board.

FUNCTIONS OF THE BOARD

SEC. 102. The Board shall—

(1) publish an annual Data Base Directory of the

United States containing the name and characteristics of each personal information system;

(2) consult with the heads of appropriate departments, agencies, and instrumentalities of the Government in accordance with section 103(5) of this Act;

(3) make rules to assure compliance with title II of this Act; and

(4) perform or cause to be performed such research activities as may become necessary to implement title II of this Act, and to assist organizations in complying with the requirements of such title.

POWERS OF THE BOARD

SEC. 103. (a) The Board is authorized—

(1) to be granted admission at reasonable hours to premises where any information system is kept or where computers or equipment or recordings for automatic data processing are kept, and may, by subpena, compel the production of documents relating to such information system or such processing as is necessary to carry out its functions, except that the production of personal information shall not be compelled without the prior consent of the data subject to which it pertains;

(2) upon the determination of a violation of any provision of this Act or regulation promulgated under

this Act, to, after opportunity for a hearing, order the organization violating such provision to cease and desist such violation;

(3) to delegate its authority under this title, with respect to information systems within a State or the District of Columbia, to such State or District, during such period of time as the Board remains satisfied that the authority established by such State or District to carry out the requirements of this Act in such State is satisfactorily enforcing those provisions;

(4) to conduct open, public hearings on all petitions for exceptions or exemptions from provisions, application, or jurisdiction of this Act, except that the Board shall not have authority to make such exceptions or exemptions but shall submit appropriate reports and recommendations to Congress; and

(5) to the fullest extent practicable, to consult with the heads of appropriate departments, agencies, and instrumentalities of the Government in carrying out the functions of the Board under this Act.

(b) The Board may procure such temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed $100 a day for individuals.

REPORTS

SEC. 404. The Board shall report, annually, on its activities to the Congress and the President.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, STATISTICAL REPORTING AND RESEARCH PURPOSES

SEC. 201. (a) Any Federal agency, State or local government, or any other organization maintaining an information system that includes personal information shall—

(1) collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization;

(2) collect information to the greatest extent possible from the data subject directly;

(3) establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

(4) maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

(5) make no dissemination to another system with

out (A) specifying requirements for security and the use of information exclusively for the purposes set forth in the notice required under subsection (c) including limitations on access thereto, and (B) determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed;

(6) transfer no personal information beyond the jurisdiction of the United States without specific authorization from the data subject or pursuant to a treaty or executive agreement in force guaranteeing that any foreign government or organization receiving personal information will comply with the applicable provisions of this Act with respect to such information;

(7) afford any data subject of a foreign nationality, whether residing in the United States or not, the same rights under this Act as are afforded to citizens of the United States;

(8) maintain a list of all persons having regular access to personal information in the information system;

(9) maintain a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority;

(10) take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance;

(11) establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;

(12) comply with the written request of any individual who receives a communication in the mails, over the telephone, or in person from a commercial organization, who believes that the name or address or both, of such individual is available because of its inclusion on a mailing list, to remove such name or address, or both, from such list; and

(13) collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used or disseminated in or by any information system operated by any governmetal agency, unless authorized by law.

(b)(1) Any such organizations maintaining an information system that disseminates statistical reports or research

findings based on personal information drawn from the system, or from systems of other organizations, shall—

(A) make available to any data subject or group (without revealing trade secrets) methodology and materials necessary to validate statistical analyses, and

(B) make no materials available for independent analysis without guarantees that no personal information will be used in a way that might prejudice judgments about any data subject.

(2) No Federal agency shall—

(A) require any individual to disclose for statistical purposes any personal information unless such disclosure is required by law, and such individual is informed of such requirement;

(B) request any individual to voluntarily disclose personal information unless such request is specifically authorized by law, and the individual is advised that such disclosure is voluntary;

(C) make available to any person, other than an authorized officer or employee of a Federal agency, any statistical study or reports or other compilation of information derived by mechanical or electronical means from any file containing personal information, or any manual or computer material relating thereto, except

those prepared, published, and made available for general public use; or

(D) publish statistics of taxpayer income classified, in whole or in part, on the basis of a coding system for the delivery of mail.

(c) Any such organization maintaining or proposing to establish an information system for personal information shall—

(1) give notice of the existence and character of each existing system once a year to the Federal Privacy Board;

(2) give public notice of the existence and character of each existing system each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations in local or regional printed media likely to bring attention to the existence of the records to data subjects;

(3) publish such annual notices for all its existing systems simultaneously;

(4) in the case of a new system, or the substantial modification of an existing system, shall give public notice and notice to the Federal Privacy Board within a reasonable time but in no case less than three months, in advance of the initiation or modification to assure indi-

viduals who may be affected by its operation a reasonable opportunity to comment; and

(5) assure that public notice given under this subsection specifies the following:

(A) the name of the system;

(B) the general purposes of the system;

(C) the categories of personal information and approximate number of persons on whom information is maintained;

(D) the categories of information maintained, confidentiality requirements, and access controls;

(E) the organization's policies and practices regarding information storage, duration of retention of information, and purging of such information;

(F) the categories of information sources;

(G) a description of types of use made of information including all classes of users and the organizational relationships among them;

(H) the procedures whereby an individual may (i) be informed if he is the subject of information in the system, (ii) gain access to such information, and (iii) contest the accuracy, completeness, timeliness, pertinence, and the necessity for retention of such information;

(I) the procedures whereby an individual or

group can gain access to the information system used for statistical reporting or research in order to subject them to independent analysis; and

(J) the business address and telephone number of the person immediately responsible for the system.

(d) Any such organization maintaining personal information shall—

(1) inform any individual asked to supply personal information whether such individual is required by law, or may refuse, to supply the information requested, and also of any specific consequences which are known to the organization, of providing or not providing such information;

(2) request permission of a data subject to disseminate part or all of such information to another organization or system not having regular access authority, and indicate the use for which such information is intended, and the specific consequences for the individual, which are known to the organization, of providing or not providing such permission;

(3) upon request and proper identification of any individual who is a data subject, grant such individual the right to inspect, in a form comprehensible to such individual—

(A) all personal information about that individual except that, in the case of medical information, such information shall, upon written authorization, be given to a physician designated by the individual;

(B) the nature of the sources of the information; and

(C) the recipients of personal information about such individual including the identity of all persons and organizations involved and their relationship to the system when not having regular access authority;

(4) at a minimum, make disclosures which are required by this Act to individuals who are data subjects—

(A) during normal business hours;

(B) in person, if the data subject appears in person and furnishes proper identification, or by mail, if the data subject has made a written request, with proper identification, at reasonable standard charges for document search and duplication; and

(C) permit the data subject to be accompanied by one person of his choosing, who must furnish reasonable identification, except that an organization may require the data subject to furnish a writ-

ten statement granting permission to the organization to discuss that individual's file in such person's presence;

(5) upon receipt of notice from any individual who is a data subject, that such individual wishes to challenge, correct, or explain information about him in such system—

(A) investigate and record the current status of such personal information;

(B) purge any such information that is found to be incomplete, inaccurate, not pertinent, not timely nor necessary to be retained, or can no longer be verified;

(C) accept and include in the record of such information, if the investigation does not resolve the dispute, any statement (not more than two hundred words in length) provided by such individual setting forth his position on such disputed information;

(D) in any subsequent dissemination or use of disputed information, clearly note that such information is disputed and supply the statement of such individual together with such information;

(E) make clear and conspicuous disclosure to

such individual of his right to make a request under this paragraph;

(F) at the request of such individual, following any correction or purging of personal information, furnish to past recipients of such information notification that the item has been purged or corrected; and

(G) in the case of a failure to resolve a dispute, advise such individual of his right to request the assistance of the Federal Privacy Board.

(c) Each such organization maintaining a personal information system on the date of the enactment of this Act shall notify by mail each data subject of the fact not later than two years following the date of enactment of this Act, at the last known address of the subject. Such notice shall—

(1) describe the type of information held in such system or systems, expected uses allowed or contemplated; and

(2) provide the name and full address of the place where the data subject may obtain personal information pertaining to him, and in the system.

(f) Data subjects of archival-type inactive files, records, or reports shall be notified by mail of the reactivation, accessing, or reaccessing of such files, records, or reports not later than six months after the date of the enactment of this Act.

(g) The requirements of subsections (a) (3) and (4) and subsections (c) and (d) (1) and (2) of this section shall not apply to any organization that (1) maintains an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of other organizations, (2) purges the names, personal numbers, or other identifying particulars of individuals, and (3) certifies to the Federal Privacy Board that no inferences may be drawn about any individual.

EXEMPTIONS

SEC. 202. The provisions of this title shall not apply to personal information systems—

(1) to the extent that information in such systems is maintained by a Federal agency, and the head of that agency determines that the release of the information would seriously damage national defense;

(2) which are part of active criminal investigatory files compiled by Federal, State, or local law enforcement organizations, except where such files have been maintained for a period longer than is necessary to commence criminal prosecution; or

(3) maintained by the press and news media, except information relating to employees of such organizations.

USE OF SOCIAL SECURITY NUMBER

SEC. 203. It shall be unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual (except to the extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program established under title II of the Social Security Act) in whole or in part because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by law.

TITLE III—MISCELLANEOUS

DEFINITIONS

SEC. 301. As used in this Act—

(1) the term "Board" means the Federal Privacy Board;

(2) the term "information system" means the total components and operations of a recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars;

(3) the term "personal information" means all in-

formation that describes, locates or indexes anything about an individual including his education, financial transactions, medical history, criminal, or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

(4) the term "data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system;

(5) the term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means;

(6) the term "organization" means any Federal agency; the government of the District of Columbia; any authority of any State, local government, or other jurisdiction; any public or private entity engaged in business for profit, as relates to that business;

(7) the term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization; and

(8) the term "Federal agency" means any depart-

ment, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof.

TRADE SECRETS

SEC. 302. In connection with any dispute over the application of any provision of this Act, no organization shall reveal any personal information or any professional, proprietary, or business secrets: except as is required under this Act. All disclosures so required shall be regarded as confidential by those to whom they are made.

CRIMINAL PENALTY

SEC. 303. Any organization or responsible officer of an organization who willfully—

(1) keeps an information system without having notified the Federal Privacy Board; or

(2) issues personal information in violation of this Act;

shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 304. (a) The Attorney General of the United States, on the advice of the Federal Privacy Board, or any aggrieved person, may bring an action in the appropriate United States district court against any person who has engaged, is engaged, or is about to engage in any acts or prac-

tices in violation of the provisions of this Act or rules of the Federal Privacy Board, to enjoin such acts or practices.

(b) Any person who violates the provisions of this Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

(1) any actual damages sustained by an individual;

(2) punitive damages where appropriate;

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

The United States consents to be sued under this section without limitation on the amount in controversy.

JURISDICTION OF DISTRICT COURTS

SEC. 305. The district courts of the United States have jurisdiction to enforce any subpena or order issued by the Federal Privacy Board under sections 102 or 103, respectively, of this Act.

RIGHT OF ACTION

SEC. 306. (a) Any individual who is denied access to information required to be disclosed under the provisions of this Act is entitled to judicial review of the grounds for such denial.

(b) The district courts of the United States have juris-

~~diction to hear and determine civil actions brought under subsection (a) of this section.~~

~~EFFECTIVE DATE~~

~~SEC. 307. This Act shall take effect one year after the date of its enactment.~~

~~AUTHORIZATION OF APPROPRIATIONS~~

~~SEC. 308. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.~~

TITLE I—PRIVACY PROTECTION COMMISSION

ESTABLISHMENT OF COMMISSION

SEC. 101. (a) There is established as an independent agency of the executive branch of the Government the Privacy Protection Commission.

(b)(1) The Commission shall be composed of five members who shall be appointed by the President, by and with the advice and consent of the Senate, from among members of the public at large who, by reason of their knowledge and expertise in any of the following areas: civil rights and liberties, law, social sciences, and computer technology, business, and State and local government, are well qualified for service on the Commission and who are not otherwise officers or employees of the United States. Not more than three of the members of the Commission shall be adherents of the same political party.

(2) One of the Commissioners shall be appointed Chairman by the President.

(3) A Commissioner appointed as Chairman shall serve as Chairman until the expiration of his term as a Commissioner of the Commission (except that he may continue to serve as Chairman for so long as he remains a Commissioner and his successor as Chairman has not taken office). An individual may be appointed as a Commissioner at the same time he is appointed Chairman.

(c) The Chairman shall preside at all meetings of the Commission and a quorum for the transaction of business shall consist of at least three members present (but the Chairman may designate an Acting Chairman who may preside in the absence of the Chairman). Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information relating to the performance of his duties or responsibilities, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or Acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, persons, or the public, and, on behalf of the Commission, shall see to the faithful execution of the policies and decisions of the Commission, and shall report thereon to the

63-619 O - 76 - 9

Commission from time to time or as the Commission may direct.

(d) Each Commissioner shall be compensated at the rate provided for under section 5314 of title 5 of the United States Code, relating to level IV of the Executive Schedule.

(e) Commissioners shall serve for terms of three years. No Commissioner may serve more than two terms. Vacancies in the membership of the Commission shall be filled in the same manner in which the original appointment was made.

(f) Vacancies in the membership of the Commission, as long as there are three Commissioners in office, shall not impair the power of the Commission to execute the functions and powers of the Commission.

(g) The members of the Commission shall not engage in any other employment during their tenure as members of the Commission.

PERSONNEL OF THE COMMISSION

SEC. 102. (a)(1) The Commission shall appoint an Executive Director who shall perform such duties as the Commission may determine. Such appointment may be made without regard to the provisions of title 5, United States Code.

(2) The Executive Director shall be compensated at a rate not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of title 5, United States Code.

(b) The Commission is authorized to appoint and fix the compensation of such officers and employees, and prescribe their functions and duties, as may be necessary to carry out the provisions of this Act.

(c) The Commission may obtain the services of experts and consultants in accordance with the provisions of section 3109 of title 5, United States Code.

FUNCTIONS OF THE COMMISSION

SEC. 103. (a) The Commission shall—

(1) publish annually a United States Directory of Information Systems containing the information specified to provide notice under section 201(c)(3) of this Act for each information system subject to the provisions of this Act and a listing of all statutes which require the collection of such information by a Federal agency;

(2) investigate, determine, and report any violation of any provision of this Act (or any regulation adopted pursuant thereto) to the President, the Attorney General, the Congress, and the General Services Administration where the duties of that agency are involved, and to the Comptroller General when it deems appropriate; and

(3) develop model guidelines for the implementation of this Act and assist Federal agencies in preparing regulations and meeting technical and administrative requirements of this Act.

(b) Upon receipt of any report required of a Federal agency describing (1) any proposed information system or data bank, or (2) any significant expansion of an existing information system or data bank, integration of files, programs for records linkage within or among agencies, or centralization of resources and facilities for data processing, the Commission shall—

(A) review such report to determine (i) the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the confidentiality of information relating to such individuals, and (ii) its effect on the preservation of the constitutional principles of federalism and separation of powers; and

(B) submit findings and make recommendations to the President, Congress, and the General Services Administration concerning the need for legislative authorization and administrative action relative to any such proposed activity in order to meet the purposes and requirements of this Act.

(c) After receipt of any report required under subsection (b), if the Commission determines and reports to the Congress that a proposal to establish or modify a data bank or information system does not comply with the standards established by or pursuant to this Act, the Federal agency submitting such report shall not proceed to establish or modify

any such data bank or information system for a period of sixty days from the date of receipt of notice from the Commission that such data bank or system does not comply with such standards.

(d) In addition to its other functions the Commission shall—

(1) to the fullest extent practicable, consult with the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out the provisions of this Act and in conducting the study required by section 106 of this Act;

(2) perform or cause to be performed such research activities as may be necessary to implement title II of this Act, and to assist Federal agencies in complying with the requirements of such title; and

(3) determine what specific categories of information should be prohibited by statute from collection by Federal agencies on the basis that the collection of such information would violate an individual's right of privacy.

CONFIDENTIALITY OF INFORMATION

SEC. 104. (a) Each department, agency, and instrumentality of the executive branch of the Government, including each independent agency, shall furnish to the Commission, upon request made by the Chairman, such data, reports, and

other information as the Commission deems necessary to carry out its functions under this Act.

(b) In carrying out its functions and exercising its powers under this Act, the Commission may accept from any Federal agency or other person any identifiable personal data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall provide appropriate safeguards to insure that the confidentiality of such information is maintained and that upon completion of the purpose for which such information is required it is destroyed or returned to the agency or person from which it is obtained, as appropriate.

POWERS OF THE COMMISSION

SEC. 105. (a)(1) The Commission may, in carrying out its functions under this Act, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such mem-

ber. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2) In case of disobedience to a subpena issued under paragraph (1) of this subsection, the Commission may invoke the aid of any district court of the United States in requiring compliance with such subpena. Any district court of the United States within the jurisdiction where such person is found or transacts business may, in case of contumacy or refusal to obey a subpena issued by the Commission, issue an order requiring such person to appear and testify, to produce such books, records, papers, correspondence, and documents, and any failure to obey the order of the court shall be punished by the court as a contempt thereof.

(3) Appearances by the Commission under this Act *shall be in its own name. The Commission shall be represented by attorneys designated by it.*

(4) Section 6001(1) of title 18, United States Code, is amended by inserting immediately after "Securities and Exchange Commission," the following: "the Privacy Protection Commission,".

(b) The Commission may delegate any of its functions to such officers and employees of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(c) In order to carry out the provisions of this Act, the Commission is authorized—

(1) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(2) to adopt, amend, and repeal interpretative rules for the implementation of the rights, standards, and safeguards provided under this Act;

(3) to enter into contracts or other arrangements or modifications thereof, with any government, any agency or department of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(4) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529);

(5) receive complaints of violations of this Act and regulations adopted pursuant thereto; and

(6) to take such other action as may be necessary to carry out the provisions of this Act.

COMMISSION STUDY OF OTHER GOVERNMENTAL AND PRIVATE ORGANIZATIONS

SEC. 106. (a)(1) The Commission shall make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information, and to determine the extent to which those standards and procedures achieve the purposes of this Act.

(2) The Commission periodically shall report its findings to the President and the Congress and shall complete the study required by this section not later than three years from the date this Act becomes effective.

(3) The Commission shall recommend to the President and the Congress the extent, if any, to which the requirements and principles of this Act should be applied to the information practices of those organizations by legislation, administrative action, or by voluntary adoption of such requirements and principles. In addition, it shall submit such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

(b)(1) In the course of such study and in its reports, the Commission shall examine and analyze—

(A) interstate transfer of information about individuals which is being undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the implied or explicitly recognized confidentiality of such information.

(2) The Commission shall include in its examination information activities in the following areas: medical, insurance, education, employment and personnel, credit, banking and financial institutions, credit bureaus, the commer-

cial reporting industry, travel, hotel, and entertainment reservations, and electronic check processing. The Commission may study such other information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

(3) In conducting the study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) conduct a thorough examination of standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information;

(D) to the maximum extent practicable, collect and utilize findings, reports, and recommendations of major governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the

problems under study by the Commission; and

(E) receive and review complaints with respect to any matter under study by the Commission which may be submitted by any person.

REPORTS

SEC. 107. The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this Act.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, INTELLIGENCE, STATISTICAL-REPORTING, AND RESEARCH PURPOSES

SEC. 201. (a) Each Federal agency shall—

(1) collect, solicit, and maintain only such personal information as is relevant and necessary to accomplish a statutory purpose of the agency;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs; and

(3) inform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, will result from nondisclosure, and what rules of confidentiality will govern the information.

(b) Each Federal agency that maintains an information system or file shall, with respect to each such system or file—

(1) insure that personal information maintained in or disseminated from the system or file is, to the maximum extent possible, accurate, complete, timely, and relevant to the needs of the agency,

(2) refrain from disclosing any such personal information within the agency other than to officers or employees who have a need for such personal information in the performance of their duties for the agency;

(3) maintain a list of all categories of persons authorized to have regular access to personal information in the system or file;

(4) maintain an accurate accounting of the date, nature, and purpose of all other access granted to the system or file, and all other disclosures of personal information made to any person outside the agency, or to another agency, including the name and address of the person or other agency to whom disclosure was made or

access was granted, except as provided by section 202(b) of this Act;

(5) establish rules of conduct and notify and instruct each person involved in the design, development, operation, or maintenance of the system or file, or the collection, use, maintenance, or dissemination of information about an individual, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance;

(6) establish appropriate administrative, technical and physical safeguards to insure the security of the information system and confidentiality of personal information and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom personal information is maintained; and

(7) establish no program for the purpose of collecting or maintaining information describing how individuals exercise rights guaranteed by the first amendment unless the head of the agency specifically determines that such program is required for the administration of a statute which the agency is charged with administering or implementing.

(c) Any Federal agency that maintains an information system or file shall—

(1) make available for distribution upon the request of any person a statement of the existence and character of each such system or file;

(2) on the date on which this Act becomes effective and annually thereafter, notify the Commission and give public notice of the existence and character of each existing system or file simultaneously, and cause such notice to be published in the Federal Register; and

(3) include in such notices at least the following information:

(A) name and location of the system or file;

(B) nature and purposes of the system or file;

(C) categories of individuals on whom personal information is maintained and categories of personal information generally maintained in the system or file, including the nature of the information and the approximate number of individuals on whom information is maintained;

(D) the confidentiality requirements and the extent to which access controls apply to such information;

(E) categories of sources of such personal information;

(F) the Federal agency's policies and practices regarding implementation of sections 201 and 202 of this Act, information storage, duration of retention of information, and elimination of such information from the system or file;

(G) uses made by the agency of the personal information contained in the system or file;

(H) identity of other agencies and categories of persons to whom disclosures of personal information are made, or to whom access to the system or file may be granted, together with the purposes therefor and the administrative constraints, if any, on such disclosures and access, including any such constraints on redisclosure;

(I) procedures whereby an individual can (i) be informed if the system or file contains personal information pertaining to himself or herself, (ii) gain access to such information, and (iii) contest the accuracy, completeness, timeliness, relevance, and necessity for retention of the personal information; and

(J) name, title, official address, and telephone number of the officer immediately responsible for the system or file.

(d)(1) Each Federal agency that maintains an information system or file shall assure to an individual upon request the following rights:

(A) to be informed of the existence of any personal information pertaining to that individual;

(B) to have full access to and right to inspect the personal information in a form comprehensible to the individual;

(C) to know the names of all recipients of information about such individual including the recipient organization and its relationship to the system or file, and the purpose and date when distributed, unless such information is not required to be maintained pursuant to this Act;

(D) to know the sources of the personal information, or where the confidentiality of such sources is required by statute, the right to know the nature of such sources;

(E) to be accompanied by a person chosen by the individual inspecting the information, except that an agency or other person may require the individual to furnish a written statement authorizing discussion of that individual's file in the person's presence;

(F) to receive such required disclosures and at reasonable standard charges for document duplication,

63-619 O - 76 - 10

in person or by mail, if upon written request, with proper identification; and

(G) to be completely informed about the uses and disclosures made of any such information contained in any such system or file except those uses and disclosures made pursuant to law or regulation permitting public inspection or copying.

(2) Upon receiving notice that an individual wishes to challenge, correct, or explain any personal information about him in a system or file, such Federal agency shall comply promptly with the following minimum requirements:

(A) investigate and record the current status of the personal information;

(B) correct or eliminate any information that is found to be incomplete, inaccurate, not relevant, not timely or necessary to be retained, or which can no longer be verified;

(C) accept and include in the record of such information, if the investigation does not resolve the dispute, any statement of reasonable length provided by the individual setting forth his position on the disputed information;

(D) in any subsequent dissemination or use of the disputed information, clearly report the challenge and supply any supplemental statement filed by the individual;

(E) at the request of such individual, following any correction or elimination of challenged information, inform past recipients of its elimination or correction; and

(F) upon a failure to resolve a dispute over information in a system or file, at the request of such individual, grant a hearing before an official of the agency, which shall be conducted as follows:

(i) such hearing shall be held within thirty days of the request at which time the individual may appeal with counsel, present evidence, and examine and cross-examine witnesses;

(ii) any record found after such a hearing to be incomplete, inaccurate, not relevant, not timely nor necessary to be retained, or which can no longer be verified, shall within thirty days of the date of such findings be appropriataely modified or purged; and

(iii) the action or inaction of any agency on a request to review and challenge personal data in its possession as provided by this section shall be reviewable by the appropriate United States district court.

(e) When a Federal agency provides by a contract, grant, or agreement the specific creation or substantial altera-

tion of an information system or file and the primary purpose of the grant, contract, or agreement is the creation or substantial alteration of such an information system or file, the agency shall, consistent with its authority, cause the requirements of subsections (a), (b), (c), and (d) to be applied to such system or file. In cases when contractors and grantees or parties to an agreement are public agencies of States or the District of Columbia or public agencies of political subdivisions of States, the requirements of subsections (a), (b), (c), and (d) shall be deemed to have been met if the Federal agency determines that the State or the District of Columbia or public agencies of political subdivisions of the State have adopted legislation or regulations which impose similar requirements.

(f)(1) Any Federal agency maintaining or proposing to establish a personal information system or file shall prepare and submit a report to the Commission, the General Services Administration, and to the Congress on proposed data banks and information systems or files, the proposed significant expansion of existing data banks and information systems or files, integration of files, programs for records linkage within or among agencies, or centralization of resources and facilities for data processing, which report shall include—

(A) the effects of such proposals on the rights, benefits, and privileges of the individuals on whom personal information is maintained;

(B) a statement of the software and hardware features which would be required to protect security of the system or file and confidentality of information;

(C) the steps taken by the agency to acquire such features in their systems, including description of consultations with representatives of the National Bureau of Standards; and

(D) a description of changes in existing interagency or intergovernmental relationships in matters involving the collection, processing, sharing, exchange, and dissemination of personal information.

(2) The Federal agency shall not proceed to implement such proposal for a period of sixty days from date of receipt of notice from the Commission that the proposal does not comply with the standards established under or pursuant to this Act.

(g) Each Federal agency covered by this Act which maintains an information system or file shall make reasonable efforts to serve advance notice on an individual before any personal information on such individual is made available to any person under compulsory legal process.

(h) No person may condition the granting or withholding of any right, privilege, or benefit, or make as a condition of employment the securing by any individual of any information which such individual may obtain through the exercise of any right secured under the provisions of this section.

DISCLOSURE OF INFORMATION

SEC. 202. (a) No Federal agency shall disseminate personal information unless—

(1) it has made written request to the individual who is the subject of the information and obtained his written consent;

(2) the recipient of the personal information has adopted rules in conformity with this Act for maintaining the security of its information system and files and the confidentiality of personal information contained therein; and

(3) the information is to be used only for the purposes set forth by the sender or the recipient pursuant to the requirements for notice under this Act.

(b) Section 201(b)(4) and section 202(a)(1) shall not apply when disclosure would be—

(1) to those officers and employees of that agency who have a need for such information in ordinary course of the performance of their duties;

(2) to the Bureau of the Census for purposes of

planning or carrying out a census or survey pursuant to the provisions of title 13, United States Code;

(3) where the agency determines that the recipient of such information has provided advance adequate written assurance that the information will be used solely as a statistical research or reporting record, and is to be transferred in a form that is not individually identifiable; or

(4) pursuant to a showing of compelling circumstances affecting health, safety, or identification of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.

(c) Section 202(a) (1), (2), and (3) and section 201 (b)(4) shall not apply when disclosure would be required or permitted pursuant to subchapter II of chapter 5 of title 5 of the United States Code (commonly known as the Freedom of Information Act of 1966).

(d) Section 201(b)(4) and paragraphs (1), (2), and (3) of subsection (a) of this section shall not apply when disclosure would be to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office. Nothing in this Act shall impair access by the Comptroller General, or any of his authorized representatives, to records maintained by an agency, including records of personal information, in the course of performance of such duties.

(e)(1) Nothing in this section shall be construed to limit the efforts of the Government pursuant to the provisions of chapter 35, title 44 of the United States Code (commonly known as the Federal Reports Act) or any other statute, to reduce the burden on citizens of collecting information by means of combining or eliminating unnecessary reports, questionnaires, or requests for information.

(2) Nothing in this section shall be construed to affect restrictions on the exchange of information between agencies as required by chapter 35, title 44 of the United States Code (commonly known as the Federal Reports Act).

(f) Subsection (a)(1) of this section shall not apply when disclosure would be to another agency or to an instrumentality of any governmental jurisdiction for a law enforcement activity if such activity is authorized by statute and if the head of such agency or instrumentality has made a written request to or has an agreement with the agency which maintains the system or file specifying the particular portion of the information desired and the law enforcement activity for which the information is sought.

EXEMPTIONS

SEC. 203. (a) The provisions of section 201(c)(3)(E), (d), and section 202, shall not apply to any personal information contained in any information system or file if the head of the Federal agency determines, in accordance with the provisions of this section, that the applica-

tion of the provisions of any of such sections would seriously damage national defense or foreign policy, where the application of any of such provisions would seriously damage or impede the purpose for which the information is maintained.

(b) The provisions of section 201(d) and section 202 shall not apply to law enforcement intelligence information or investigative information if the head of the Federal agency determines, in accordance with the provisions of any of such sections would seriously damage or impede the purpose for which the information is maintained: Provided, That investigative information may not be exempted under this section where such information has been maintained for a period longer than is necessary to commence criminal prosecution. Nothing in this Act shall prohibit the disclosure of such investigative information to a party in litigation where required by statute or court rule.

(c)(1) A determination to exempt any such system, file, or information may be made by the head of any such agency in accordance with the requirements of notice, publication, and hearing contained in sections 553 (b), (c), and (e), 556, and 557 of title 5, United States Code. In giving notice of an intent to exempt any such system, file, or information, the head of such agency shall specify the nature and purpose of the system, file, or information to be exempted.

(2) Whenever any Federal agency undertakes to exempt any information system, file, or information from the provi-

sions of this Act, the head of such Federal agency shall promptly notify the Commission of its intent and afford the Commission opportunity to comment.

(3) The exception contained in section 553(d) of title 5, United States Code (allowing less than thirty days' notice), shall not apply in any determination made or any proceeding conducted under this section.

ARCHIVAL RECORDS

SEC. 204. (a) Federal agency records which are accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44, United States Code, shall, for the purposes of this section, be considered to be maintained by the agency which deposited the records and shall be subject to the provisions of this Act. The Administrator of General Services shall not disclose such records, or any information therein, except to the agency which maintains the records or pursuant to rules established by that agency.

(b) Federal agency records pertaining to identifiable individuals which were transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government shall for the purposes of this Act, be considered to be maintained by the National Archives and shall not be subject to the provisions of this Act except section 201(b) (5) and (6).

(c) The National Archives shall, on the date on which this Act becomes effective and annually thereafter, notify the Commission and give public notice of the existence and character of the information systems and files which it maintains, and cause such notice to be published in the Federal Register. Such notice shall include at least the information specified under section 201(c)(3) (G), (I), and (J).

EXCEPTIONS

SEC. 205. (a) No officer or employee of the executive branch of the Government shall rely on any exemption in subchapter II of chapter 5 of title 5 of the United States Code (commonly known as the Freedom of Information Act) to withhold information relating to an individual otherwise accessible to an individual under this Act.

(b) Nothing in this Act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder.

(c) The provisions of section 201(d)(1) of this Act shall not apply to records collected or furnished and used by the Bureau of the Census solely for statistical purposes or as authorized by section 8 of title 13 of the United States Code.

MAILING LISTS

SEC. 206. (a) An individual's name and address may

not be sold or rented by a Federal agency unless such action is specifically authorized by law. This provision shall not be construed to require the confidentiality of names and addresses otherwise permitted to be made public.

(b) Upon written request of any individual, any person engaged in interstate commerce who maintains a mailing list shall remove the individual's name and address from such list.

TITLE III—MISCELLANEOUS

DEFINITIONS

SEC. 301. As used in this Act—

(1) the term "Commission" means the Privacy Protection Commission;

(2) the term "personal information" means any information that identifies or describes any characteristic of an individual, including, but not limited to, his education, financial transactions, medical history, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or

membership in an organization or activity, or admission to an institution;

(3) the term "individual" means a citizen of the United States or an alien lawfully admitted through permanent residence;

(4) the term "information system" means the total components and operations, whether automated or manual, by which personal information, including name or identifier, is collected, stored, processed, handled, or disseminated by an agency;

(5) the term "file" means a record or series of records containing personal information about individuals which may be maintained within an information system;

(6) the term "data bank" means a file or series of files pertaining to individuals;

(7) the term "Federal agency" means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof;

(8) the term "investigative information" means information associated with an identifiable individual compiled by—

(A) an agency in the course of conducting a criminal investigation of a specific criminal act where such investigation is pursuant to a statutory function of the agency. Such information may pertain to that criminal act and be derived from reports of informants and investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically and expressly required by State or Federal statute to be made public; or

(B) by an agency with regulatory jurisdiction which is not a law enforcement agency in the course of conducting an investigation of specific activity which falls within the agency's regulatory jurisdiction. For the purposes of this paragraph, an "agency with regulatory jurisdiction" is an agency which is empowered to enforce any Federal statute or regulation, the violation of which subjects the violator to criminal or civil penalties;

(9) the term "law enforcement intelligence information" means information associated with an identifiable individual compiled by a law enforcement agency in the course of conducting an investigation of an

individual in anticipation that he may commit a specific criminal act, including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically by incident and expressly required by State or Federal statute to be made public;

(10) the term "criminal history information" means information on an individual consisting of notations of arrests, detentions, indictments, informations, or other formal criminal charges and any disposition arising from those arrests, detentions, indictments, informations, or charges. The term shall not include an original book of entry or police blotter maintained by a law enforcement agency at the place of an original arrest or place of detention, indexed chronologically and required to be made public, nor shall it include court records of public criminal proceedings indexed chronologically; and

(11) the term "law enforcement agency" means an agency whose employees or agents are empowered by State or Federal law to make arrests for violations of State or Federal law.

CRIMINAL PENALTY

SEC. 302. (a) Any officer or employee of any Federal agency who willfully keeps an information system without meeting the notice requirements of this Act set forth in section 201(c) shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

(b) Whoever, being an officer or employee of the Commission, shall disseminate any personal information about any individual obtained in the course of such officer or employee's duties in any manner or for any purpose not specifically authorized by law shall be fined not more than $10,000, or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 303. (a) Any individual who is denied access to information required to be disclosed under the provisions of this Act may bring a civil action in the appropriate district court of the United States for damages or other appropriate relief against the Federal agency which denied access to such information.

(b) The Attorney General of the United States, or any aggrieved person, may bring an action in the appropriate United States district court against any person who has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this Act, to enjoin such acts or practices.

(c) Any person who violates the provisions of this Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

(1) any actual damages sustained by an individual;

(2) punitive damages where appropriate; and

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(d) The United States consents to be sued under this section without limitation on the amount in controversy.

JURISDICTION OF DISTRICT COURTS

SEC. 304. (a) The district courts of the United States have jurisdiction to hear and determine civil actions brought under section 303 of this Act and may examine the information in camera to determine whether such information or any part thereof may be withheld under any of the exemptions in section 203 of this Act. The burden is on the Federal agency to sustain such action.

(b) In any action to obtain judicial review of a decision to exempt any personal information from any provision of this Act, the court may examine such information in camera to determine whether such information or any part

63-619 O - 76 - 11

thereof is properly classified with respect to national defense, foreign policy or law enforcement intelligence information or investigative information and may be exempted from any provision of this Act. The burden is on the Federal agency to sustain any claim that such information may be so exempted.

EFFECTIVE DATE

SEC. 305. This Act shall become effective one year after the date of enactment except that the provisions of title I of this Act shall become effective on the date of enactment.

AUTHORIZATION OF APPROPRIATIONS

SEC. 306. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.

Amend the title so as to read: "A bill to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes."

Calendar No. 1127

93D CONGRESS
2d Session

SENATE

REPORT
No. 93-1183

PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE AND DISCLOSURE OF INFORMATION

REPORT

OF THE

COMMITTEE ON GOVERNMENT OPERATIONS UNITED STATES SENATE

TO ACCOMPANY

S. 3418

TO ESTABLISH A PRIVACY PROTECTION COMMISSION, TO PROVIDE MANAGEMENT SYSTEMS IN FEDERAL AGENCIES AND CERTAIN OTHER ORGANIZATIONS WITH RESPECT TO THE GATHERING AND DISCLOSURE OF INFORMATION CONCERNING INDIVIDUALS, AND FOR OTHER PURPOSES



SEPTEMBER 26, 1974.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1974

COMMITTEE ON GOVERNMENT OPERATIONS

SAM J. ERVIN, JR., North Carolina, *Chairman*

JOHN L. McCLELLAN, Arkansas
HENRY M. JACKSON, Washington
EDMUND S. MUSKIE, Maine
ABRAHAM RIBICOFF, Connecticut
LEE METCALF, Montana
JAMES B. ALLEN, Alabama
LAWTON CHILES, Florida
SAM NUNN, Georgia
WALTER D. HUDDLESTON, Kentucky

CHARLES H. PERCY, Illinois
JACOB K. JAVITS, New York
EDWARD J. GURNEY, Florida
WILLIAM V. ROTH, JR., Delaware
BILL BROCK, Tennessee

ROBERT BLAND SMITH, Jr., *Chief Counsel and Staff Director*
ELI E. NOBLEMAN, *Counsel*
W. P. GOODWIN, Jr., *Counsel*
J. ROBERT VASTINE, *Minority Counsel*
BRIAN CONBOY, *Special Counsel to the Minority*
W. THOMAS FOXWELL, *Staff Editor*

MARCIA J. MacNAUGHTON, *Chief Consultant*
Dr. ALAN F. WESTIN, *Special Consultant*
Dr. CHRISTOPHER H. PYLE, *Consultant*
MARK BRAVIN, *Consultant*

(II)

CONTENTS

	Page
Purpose	1
Background	3
General statement	14
Coverage	17
Right of access and challenge	20
Law enforcement files	22
Privacy Commission	23
Enforcement	27
Social Security numbers	28
Mailing lists	31

SECTION-BY-SECTION ANALYSIS

TITLE I—PRIVACY PROTECTION COMMISSION:	
Section 101—Establishment of Commission	33
Section 102—Personnel of the Commission	34
Section 103—Functions of the Commission	34
Section 104—Confidentiality of information	38
Section 105—Powers of the Commission	38
Section 106—Commission study of other governmental and private organizations	39
Section 107—Reports	44
TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS:	
Section 201—Safeguard requirements for administrative, intelligence, statistical-reporting, and research purposes	45
Section 202—Disclosure of information	68
Disclosure exceptions	70
Section 203—Exemptions	74
Section 204—Archival records	76
Section 205—Exceptions	77
Section 206—Mailing lists	78
TITLE III—MISCELLANEOUS:	
Section 301—Definitions	78
Section 302—Criminal penalty	81
Section 303—Civil remedies	82
Section 304—Jurisdiction of District Courts	83
Section 305—Effective date	84
Estimated cost of legislation	84
Rollcall vote	85

Calendar No. 1127

93D CONGRESS } SENATE } REPORT
2d Session } } No. 93-1183

PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE AND DISCLOSURE OF INFORMATION

SEPTEMBER 26, 1974.—Ordered to be printed

Mr. ERVIN, from the Committee on Government Operations, submitted the following

REPORT

[To accompany S. 3418]

The Committee on Government Operations, to which was referred the bill (S. 3418) to establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State and local governments, and other organizations regarding such information, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and an amended title and recommends that the bill as amended do pass.

PURPOSE

The purpose of S. 3418, as amended, is to promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.

It is to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government and with respect to all of its other manual or mechanized files.

It is designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies.

It is to prevent the secret gathering of information on people or the creation of secret information systems or data banks on Americans by employees of the departments and agencies of the executive branch.

It is designed to set in motion for long-overdue evaluation of the needs of the Federal Government to acquire and retain personal information on Americans, by requiring stricter review within agencies of criteria for collection and retention.

It is also to promote observance of valued principles of fairness and individual privacy by those who develop, operate, and administer other major institutional and organizational data banks of government and society.

S. 3418 Accomplishes These Purposes in Five Major Ways

First, it requires agencies to give detailed notice of the nature and uses of their personal data banks and information systems and their computer resources. It requires a new Privacy Commission to maintain and publish an information directory for the public, to examine executive branch proposals for new personal data banks and systems, and to report to Congress and the President if they adversely affect privacy and individual rights. It penalizes those who keep secret such a personal information system or data bank.

Second, the bill establishes certain minimum information-gathering standards for all agencies to protect the privacy and due process rights of the individual and to assure that surrender of personal information is made with informed consent or with some guarantees of the uses and confidentiality of the information. To this end, it charges agencies:

> To collect, solicit and maintain only personal information that is relevant and necessary for a statutory purpose of the agency;
>
> To prevent hearsay and inaccuracies by collecting information directly from the person involved as far as practicable;
>
> To inform people requested or required to reveal information about themselves whether their disclosure is mandatory or voluntary, what uses and penalties are involved, and what confidentiality guarantees surround the data once government acquires it; and
>
> To establish no program for collecting or maintaining information on how people exercise First Amendment rights without a strict reviewing process.

Third, the bill establishes certain minimum standards for handling and processing personal information maintained in the data banks and systems of the executive branch, for preserving the security of the computerized or manual system, and for safeguarding the confidentiality of the information. To this end, it requires every department and agency to insure, by whatever steps they deem necessary:

> That the information they keep, disclose, or circulate about citizens is as accurate, complete, timely, and relevant to the agency's needs as possible;
>
> That they refrain from disclosing it unless necessary for employee duties, or from making it available outside the agency

without the consent of the individual and proper guarantees, unless pursuant to open records laws, or unless it is for certain law enforcement or other purposes;

That they take certain administrative actions to keep account of the employees and people and organizations who have access to the system or file, and to keep account of the disclosures and uses made of the information;

That they establish rules of conduct with regard to theiethical and legal obligations in developing and operating a computerized or other data system and in handling personal data, and take action to instruct all employees of such duties;

That they not sell or rent the names and addresses of people whose files they hold; and

That they issue appropriate administrative orders, provide personnel sanctions, and establish appropriate technical and physical safeguards to insure the security of the information system and the confidentiality of the data.

Fourth, to aid in the enforcement of these legislative restraints, the bill provides administrative and judicial machinery for oversight and for civil remedy of violations. To this end, the bill:

Gives the individual the right, with certain exceptions, to be told upon request whether or not there is a government record on him or her, to have access to it, and to challenge it with a hearing upon request, and with judicial review in Federal Court;

Establishes an independent Privacy Protection Commission with subpoena power and authority to receive and investigate charges of violations of the Act and report them to the proper officials; to develop model guidelines and assist agencies in implementing the Act; and to alert the President and Congress to proposed Federal information programs and data banks which deviate from the standards and requirements of the Act; and

Judicial remedies allow the enforcement of the act through the courts by individuals and organizations in civil actions challenging denial of access to personal information or through suits by the Attorney General or any aggrieved person to enjoin violations or threatened violations of the Act.

Fifth, the bill requires the Commission to make a study of the major data banks and computerized information systems of other governmental agencies and of private organizations and to recommend any needed changes in the law governing their practices or the application of all or part of this legislation in order to protect the privacy of the individual.

Background

The Committee on Government Operations' ad hoc Subcommittee on Privacy and Information Systems conducted hearings on June 18, 19, and 20, 1974, to consider S. 3418, cosponsored by Senators Ervin, Percy, Muskie, and Ribicoff. The hearings were held jointly with the

Judiciary Committee's Subcommittee on Constitutional Rights which was considering the following legislation on related issues:

S. 2810, introduced by Senator Goldwater, to protect the constitutional right of privacy of individuals concerning whom identifying numbers or identifiable information is recorded by enacting principles of information practice in furtherance of amendments I, III, IV, X, and XIV of the U.S. Constitution;

S. 2542, introduced by Senator Bayh to protect the constitutional right of privacy of those individuals concerning whom records are maintained; and

S. 3116, introduced by Senator Hatfield, to protect the individual's right to privacy by prohibiting the sale or distribution of certain information.

Committee Oversight

These hearings continued the oversight by the Government Operations Committee of the development and proper management of automated data processing in the Federal Government and its concern for the effect on Federal-State relations of national and intergovernmental data systems involving electronic and manual transmission, sharing, and distribution of personal information about citizens.

Senator Ervin announced the joint hearings as Chairman of both subcommittees, in a Senate speech on June 11 in which he summarized the issues and described some of the complaints from citizens which have been received by Members of Congress, as follows:

> It is a rare person who has escaped the quest of modern government for information. Complaints which have come to the Constitutional Rights Subcommittee and to Congress over the course of several administrations show that this is a bipartisan issue which effects people in all walks of life. The complaints have shown that despite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information-gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy make it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.
>
> The complaints show that many Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its power to investigate and store information.
>
> They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it.
>
> They are concerned about intrusive statistical questionnaires backed by the sanctions of criminal law or the threat of it because they have been subject to these practices over a number of years.

S. 3418 provides an "Information Bill of Rights" for citizens and a "Code of Fair Information Practices" for departments and agencies of the executive branch.

Testimony and statements were received from Members of Congress who have sponsored legislation and conducted investigations into complaints from citizens; from Federal, State, and local officials including representatives of the Administration and certain departments and agencies, the Domestic Council Committee on Right to Privacy, the Commerce Department, Bureau of the Census, National Bureau of Standards, the General Services Administration, the Office of Telecommunications Policy; the National Governors Conference, the National Legislative Conference, the National Association for State Information Systems, and the Government Management Information Sciences. Many interested organizations and individuals with expert knowledge of the subject advised the Committee. These included the former Secretary of Health, Education, and Welfare, Elliot Richardson, authors of major studies, experts in computer technology, constitutional law, and public administration, the American Civil Liberties Union, Liberty Lobby, the National Committee for Citizens in Education, the American Society of Newspaper Editors, and others.

The provisions of the bill as reported, reflect the bill as introduced, with revisions based on testimony of witnesses at hearings, consultations with experts in privacy, computer technology, and law, representatives of Federal agencies and of many private organizations and businesses, as well as the staffs of a number of congressional committees engaged in investigations related to privacy and governmental information systems.

The Committee finds that the need for enactment of these provisions is supported by the investigations and recommendations of numerous congressional committees, reports of bar associations, and others organizations, and conclusions of governmental study commissions.

To cite only a few, there are:

Earlier studies of computers and information technology by the Senate Committee on Government Operations and the current hearings and studies relating to S. 3418;

The hearings and studies on computers, data banks and the bill of rights and other investigations of privacy violations before the Constitutional Rights Subcommittee;

The hearings and studies of computer privacy and government information-gathering before the Judiciary Administrative Practices Subcommittee;

The hearings on insurance industries and other data banks before the Judiciary Antitrust Subcommittee;

The hearings on abuses in the credit reporting industries and on protection of bank records before the Senate Banking, Housing and Urban Affairs Committee;

Investigations over many years by the House Government Operations Committee; and

Finally, there are many revelations during the hearings before the Select Committee on Watergate of improper access, transfer and disclosure of personal files and of unconstitutional, illegal or improper investigation of and collection of personal information on individuals.

Particularly supportive of the principles and purposes of S. 3418 are the following reports sponsored by Government agencies:

1. "Legal Aspects of Computerized Information Systems" by the Committee on Scientific and Technical Information, Federal Council of Science and Technology, 1972.

2. "Records, Computers and the Rights of Citizens". Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education and Welfare, July 1973.

3. "Databanks in a Free Society, Computers, Record-Keeping and Privacy", of the Computer Science and Engineering Board, National Academy of Sciences, by Alan F. Westin and Michael Baker.

4. Technical Reports by Project Search Law Enforcement Assistance Administration, Department of Justice.

5. A draft study by the Administrative Conference of the United States on Interagency Transfers of Information.

6. Report by the National Governors Conference.

7. Reports by international study bodies.

The ad hoc subcommittee has initiated two surveys of the Governors and of the attorneys general of the States which are producing responses supportive of congressional legislation on privacy and Federal computers and information technology. They also reveal strong efforts in State and local governments to enact similar or stronger legislation to protect privacy.

The need for the bill is also evident from the sample of legal literature and public administration articles and press articles reprinted in the appendix of the subcommittee hearings.

Finally, there are the complaints of information abuses received by many Members of Congress and diligently investigated by each of them.

Dr. Alan F. Westin, director of the 1972 National Academy of Sciences Project, reported that the study suggested "six major areas of priority for public action: laws to give individuals a right of notice, access, and challenge to virtually every file held by local, State, and national government, and most private record systems as well; promulgation of clearer rules for data-sharing and data-restriction than we now have in most important personal data files; rules to limit the collection of unnecessary and overbroad personal data by any organization; increased work by the computer industry and professionals on security measures to make it possible for organizations to keep their promises of confidentiality; limitations on the current, unregulated use of the Social Security number; and the development of independent, 'information-trust' agencies to hold especially sensitive personal data, rather than allowing these data to be held automatically by existing agencies."

Witnesses cited the failure of legislation and judicial decisions to keep pace with the growing efficiency of data usage by promulgating clear standards for data collection, data exchange, and individual access rights. Similarly, many other witnesses before Congress agreed

with his judgment that the mid-1970's is precisely the moment when such standards need to be defined and installed if the managers of large data systems, and the specialists of the computer industry, are to have the necessary policy guidelines around which to engineer the new data systems that are being designed and implemented.

Dr. Westin cautioned:

> To delay congressional action in 1974–75, therefore, is to assure that a large number of major data systems will be built, and other existing computerized systems expanded, in ways that will make it extremely costly to alter the software, change the file structures, or reorganize the data flows to respond to national standards. And beyond the money, such late changes threaten to jeopardize many operations in vital public services that will be increasingly based on computerized systems—national health insurance, family assistance plans, national criminal-offender records, and many others. In fact, these systems may become so large, so expensive, and so vital to so many Americans that public opinion will be put to a terrible choice—serious interruption of services *or* installation of citizen-rights measures.

The spread of the data bank concept, the increasing computerization of sensitive subject areas relating to people's personal lives and activities, and the tendency of government to put information technology to uses detrimental to individual privacy were detailed by Professor Arthur Miller. He stated:

> Americans today are scrutinized, measured, watched, counted, and interrogated by more governmental agencies, law enforcement officials, social scientists and poll takers than at any other time in our history. Probably in no Nation on earth is as much individualized information collected, recorded and disseminated as in the United States.
>
> The information gathering and surveillance activities of the Federal Government have expanded to such an extent that they are becoming a threat to several of every American's basic rights, the rights of privacy, speech, assembly, association, and petition of the Government.
>
> * * * * * * *
>
> I think if one reads Orwell and Huxley carefully, one realizes that "1984" is a state of mind. In the past, dictatorships always have come with hobnailed boots and tanks and machineguns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive, just as chilling and just as debilitating on our constitutional protections. I think it is this fear that presents the greatest challenge to Congress right now.

Professor Miller characterized the reported bill as "a major step in developing a rationale regulatory scheme for achieving an effective balance between a citizen and the Government in the important field of information privacy. The creation of a Privacy Protection Commission with broad power of investigation, reporting, and suasion seems to me to be an effective way of developing policy in this rapidly

changing environment. Also worthy of enthusiastic support is Title II of the proposed legislation. We simply cannot allow more time to pass without developing standards of care with regard to the gathering and handling of personal information. In that regard, S. 3418 goes a long way to establish the much needed information bill of rights."

The four-year survey by the Constitutional Rights Subcommittee, intended as an aid to Congress in evaluating pending legislation, demonstrates the need for requiring the following Congressional action:

> Explicit statutory authority for the creation of each data bank, as well as prior examination and legislative approval of all decisions to computerize files;
>
> Privacy safeguards built into the increasingly computerized government files as they are developed, rather than merely attempting to supplement existing systems with privacy protections;
>
> Notification of subjects that personal information about them is stored in a Federal data bank and provision of realistic opportunities for individual subjects to review and correct their own records;
>
> Constraints on interagency exchange of personal data about individuals and the creation of interagency data bank cooperatives;
>
> The implementation of strict security precautions to protect the data banks and the information they contain from unauthorized or illegal access; and
>
> Continued legislative control over the purposes, contents and uses of government data systems.

HEW Report

Another report reflecting major provisions of S. 3418 is that rendered by the Secretary's Advisory Committee on Automated Personal Data Systems to the Department of Health, Education and Welfare. Former Secretary Elliot Richardson described their findings in his testimony.

The report found that "concern about computer-based record keeping usually centers on its implications for personal privacy, and understandably so if privacy is considered to entail control by an individual over the uses made of information about him. In many circumstances in modern life, an individual must either surrender some of that control or forego the services that an organization provides. Although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms."

"Under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices." For this reason, as well as because of the need to establish standards of record-keeping practice appropriate to the computer age, the report recommends the enactment of a Federal "Code of Fair Information Practice" for all automated personal data systems. The Code rests on five basic prin-

ciples that would be given legal effect as "safeguard requirements" for automated personal data systems.

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.*

The Advisory Committee recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems as follows:

> The Code should define "fair information practice" as adherence to specified safeguard requirements.
>
> The Code should prohibit violation of any safeguard requirement as an "unfair information practice."
>
> The Code should provide that an unfair information practice be subject to both civil and criminal penalties.
>
> The Code should provide for injunctions to prevent violation of any safeguard requirement.
>
> The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits."

Pending the enactment of a code of fair information practice, the Advisory Committee also recommended that all Federal agencies apply these requirements to all Federal systems, and assure through formal rulemaking that they are applied to all other systems within reach of the Federal government's authority. Beyond the Federal Government, they urged that state and local governments, the institutions within reach of their authority, and all private organizations adopt the safeguard requirements by whatever means are appropriate.

Revolutionary changes in data collection, storage and sharing were described by Senator Goldwater, who was one of many witnesses who called for enactment of the recommendations of the HEW Advisory Committee. He stated:

> Computer storage devices now exist which make it entirely practicable to record thousands of millions of characters of information, and to have the whole of this always available

*"*Records, Computers, and the Rights of Citizens*," U. S. Department of Health, Education and Welfare, 1973, p. xx.

> for instant retrieval . . . Distance is no obstacle. Communications circuits, telephone lines, radio waves, even laster beams, can be used to carry information in bulk at speeds which can match the computer's own. Time-sharing is normal . . . we are now hearing of a system whereby it is feasible for there to be several thousands of simultaneous users or terminals. Details of our health, our education, our employment, our taxes, our telephone calls, our insurance, our banking and financial transactions, pension contributions, our books borrowed, our airline and hotel reservations, our professional societies, our family relationships, all are being handled by computers right now. Unless these computers, both governmental and private, are specifically programmed to erase unwanted history, these details from our past can at any time be reassembled to confront us . . . We must program the programmers while there is still some personal liberty left.

The Committee has found that the concern for privacy is a bipartisan issue and knows no political boundaries. President Ford, as Vice-President, chaired a Domestic Council Committee on the Right of Privacy which was established by President Nixon in February 1974. In recent address on the subject, he stated:

> In dealing with troublesome privacy problems, let us not, however, scapegoat the computer itself as a Frankenstein's monster. But let us be aware of the implications posed to freedom and privacy emerging from the ways we use computers to collect and disseminate personal information. A concerned involvement by all who use computers is the only way to produce standards and policies that will do the job. It is up to us to assure that information is not fed into the computer unless it is relevant.
>
> Even if it is relevant, there is still a need for discretion. A determination must be made if the social harm done from some data outweighs its usefullness. The decision-making process is activated by demands of people on the government and business for instant credit and instant services. Computer technology has made privacy an issue of urgent national significance. It is not the technology that concerns me but its abuse. I am also confident that technology capable of designing such intricate systems can also design measures to assure security.

FEDNET

In the same address, the Vice-President called attention to FEDNET and problems involved in a proposed centralization of computer facilities which concerned several Congressional committees and which provisions in S. 3418 would correct. He stated:

> The Government's General Services Administration has distributed specifications for bids on centers throughout the country for a massive new computer network. It would have the potential to store comprehensive data on individuals and institutions. The contemplated system, known as FEDNET, would link Federal agencies in a network that would allow

> GSA to obtain personal information from the files of many Federal departments. It is portrayed as the largest single governmental purchase of civilian data communication in history.
>
> I am concerned that Federal protection of individual privacy is not yet developed to the degree necessary to prevent FEDNET from being used to probe into the lives of individuals. Before building a nuclear reactor, we design the safeguards for its use. We also require environmental impact statements specifying the anticipated effect of the reactor's operation on the environment. Prior to approving a vast computer network affecting personal lives, we need a comparable privacy impact statement. We must also consider the fallout hazards of FEDNET to traditional freedoms.

Examples

The revelations before the Select Committee to Investigate Presidential Campaign Activities concerning policies and practices of promoting the illegal gathering, use or disclosure of information on Americans who disagreed with governmental policies were cited by almost all witnesses as additional reasons for immediate congressional action on S. 3418 and other privacy legislation. The representative of the American Civil Liberties Union stated:

> Watergate has thus been the symbolic catalyst of a tremendous upsurge of interest in securing the right of privacy: wiretapping and bugging political opponents, breaking and entering, enemies lists, the Huston plan, national security justifications for wiretapping and burglary, misuse of information compiled by government agencies for political purposes, access to hotel, telephone and bank records; all of these show what government can do if its actions are shrouded in secrecy and its vast information resources are applied and manipulated in a punitive, selective, or political fashion.

Despite such current concern, Congressional studies and complaints to Congress show that the threats to individual privacy from the curiosity of administrators and salacious inquiries of investigators predated "Watergate" by many years. These have been described at length in the hearing record on S. 3418.

For example, under pain of civil and criminal sanctions, many people have been selected and told to respond to questions on statistical census questionnaires such as the following:

> How much rent do you pay?
>
> Do you live in a one-family house?
>
> If a woman, how many babies have you had? Not counting still births.
>
> How much did you earn in 1967?
>
> If married more than once, how did your first marriage end?
>
> Do you have a clothes dryer?
>
> Do you have a telephone, if so, what is the number?

Do you have a home food freezer?

Do you own a second home?

Does your TV set have UHF?

Do you have a flush toilet?

Do you have a bathtub or shower?

The studies show that thousands of questionnaires are sent out yearly asking personal questions, but people are not told their responses are voluntary; many think criminal penalties attach to them; it is difficult for them to find out what legal penalties attach to a denial of the information or what will be done with it. If they do not respond, reports show that they are subjected to telephone calls, certified follow-up letters, and personal visits. Much of this work is done by the Census Bureau under contract, and many people believe that whatever agency receives the responses, their answers are subject to the same mandatory provisions and confidentiality rules as the decennial census replies. A Senate survey revealed that in 3 years alone the Census Bureau had provided their computer services at the request of 24 other agencies and departments for conducting voluntary surveys covering over 6 million people. Other independent voluntary surveys were conducted by the agencies themselves on subjects ranging from bomb shelters, to smoking habits, to birth control methods, to whether people who had died had slept with the window open. The form usually asked for social security number, address and phone number.

One such survey technique came to light through complaints to Congress from elderly, disabled or retired people in all walks of life who were pressured to answer a 15-page form sent out by the Census Bureau for the Department of Health, Education and Welfare which asked:

What have you been doing in the last 4 weeks to find work?

Taking things all together, would you say you are very happy, pretty happy, or not too happy these days?

Do you have any artificial dentures?

Do you—or your spouse—see or telephone your parents as often as once a week?

What is the total number of gifts that you give to individuals per year?

How many different newspapers do you receive and buy regularly?

About how often do you go to a barber shop or beauty salon?

What were you doing most of last week?

Applicants for Federal jobs in some agencies, and employees in certain cases, have been subjected to programs requiring them to answer forms of psychological tests which contained questions such as these:*

*Senate Report 93-724, to accompany S. 1688, "To Protect the Privacy and Rights of Federal Employees." The report describes other similar programs for soliciting, collecting or using personal information from and about applicants and employees. S. 1688 has been approved by the Senate five times.

63-619 O - 76 - 12

I am very seldom troubled by constipation.

My sex life is satisfactory.

At times I feel like swearing.

I have never been in trouble because of my sex behavior.

I do not always tell the truth.

I have no difficulty in starting or holding my bowel movements

I am very strongly attracted by members of my own sex.

I like poetry.

I go to church almost every week.

I believe in the second coming of Christ.

I believe in a life hereafter.

My mother was a good woman.

I believe my sins are unpardonable.

I have used alcohol excessively.

I loved my Mother.

I believe there is a God.

Many of my dreams are about sex matters.

At periods my mind seems to work more slowly than usual.

I am considered a liberal "dreamer" of new ways rather than a practical follower of well-tried ways. (a) true, (b) uncertain, (c) false.

When telling a person a deliberate lie, I have to look away, being ashamed to look him in the eye. (a) true, (b) uncertain, (c) false.

First Amendment Programs: the Army

Section 201(b)(7) prohibits departments and agencies from undertaking programs for gathering information on how people exercise their First Amendment rights unless certain standards are observed. Section 201(a) prevents them from collecting and maintaining information which is not relevant to a statutory purpose.

The need for these provisions have been made evident in many ways. In addition to federal programs for asking people questions such as whether they "believe in the second coming of Christ," there have been numerous other programs affecting First Amendment rights.

One of the most pervasive of the intrusive information programs which have concerned the Congress and the public in recent years involved the Army surveillance of civilians, through its own records and those of other federal agencies. The details of these practices have been documented in Congressional hearings and reports and were summarized by Senator Ervin as follows:*

*Hearings before the Subcommittee on Constitutional Rights of the Judiciary Committee, 4 *Columbia Human Events Report* 1972. Hearings, 92d Cong., 2d sess. February 1971.

Despite First Amendment rights of Americans, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.

Allegedly for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, taperecorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

With very few, if any, directives to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.

The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks.

General Statement

The premise underlying this legislation is that good government and efficient management require that basic principles of privacy, confidentiality and due process must apply to all personal information programs and practices of the Federal Government, and should apply to those of State and local government as well as to those of the organizations, agencies and institutions of the private sector.

The need for such a general legislative formula is made necessary by the haphazard patterns of information swapping among government agencies, the diversity of confidentiality rules and the unevenness of their application within and among agencies. The lack of self-restraint in information-gathering from and about citizens on the part of some agencies has demonstrated the potential throughout government for

imposing coercive information burdens on citizens or for invading areas of thought, belief or personal life which should be beyond the reach of the Federal data collector.

* * *

The myriad rules and regulations reflecting many years of ad hoc policy decisions to meet the information needs of administrators facing problems of the political moment will, under this bill, be replaced by a rule of law. The Committee emphasizes that enactment of such general legislation in no way precludes specific legislation to govern records for special programs in such areas as tax, finance, health, welfare, census, and law enforcement. Furthermore, it should not be construed as a final statement by Congress on the right of privacy and other related rights as they may be developed or interpreted by the courts.

* * *

The Committee affirms that the present statutory division of executive branch power among the departments and agencies and bureaus promotes accountability and is most conducive to legislative oversight, Presidential management, and responsiveness to the public will. We believe that the creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees would tend to defeat these purposes, and threaten the observance of the values of privacy and confidentiality in the administrative process. The Committee therefore intends in S. 3418 to require strict reporting by agencies and departments and meaningful congressional and executive branch review of any proposed use of information technology which might tend to further such negative developments.

* * *

The Committee recognizes that the computer is an instrument which is absolutely essential to the proper transaction of many government programs, and that the collection of information from the individual is absolutely necessary to carry out those programs.

Also necessary to modern government is the science of management of the many aspects of information technology and its related professional personnel which have been incorporated very rapidly into the administrative processes of the Federal Government.

At the same time, however, the Committee believes that in the management of computer systems and all other aspects of information technology, a special status must be accorded to the issue of individual privacy, that is, the right of an individual to have such gathering of personal information as may be collected by the Government confined to that for which there is a legitimate use, and then secondly, after it is gathered, to have access to that information confined to those who have a governmental end in view for its use, and thirdly, to be assured by government that there is as little leakage as possible to unauthorized persons.

The present legislation is designed to foster these goals in the administrative processes of the executive branch. The Committee believes that the bill strikes a balance between governmental needs and the personal freedoms of the individual.

The complexities and scale of modern government make it impossible for Congress or the courts to monitor every decision made which involves personal information. The bill therefore depends partly for its enforcement on the individual data subject and makes that person a participant in government's decision to exercise its information power over an individual.

* * *

The Committee is convinced that legislation cannot and should not be neutral toward the information technology by means of which the Federal Government affects individual rights. Certain kinds of information should not be collected or maintained or disclosed by government agencies because to do so is either unconstitutional, unfair, unwise, or simply bad management of the people's business. This means, furthermore, that certain computer hardware and software used to operate the information systems of government should provide features which will promote the necessary security of any part of the system and the confidentiality of the information processed and handled by means of it.

* * *

The bill does not rest solely on the findings of any one report or study, but on review and consideration of all of the studies cited here.

The Committee is convinced that effective legislation must provide standards for and limitations on the information power of government. Providing a right of access and challenge to records, while important, is not sufficient legislative solution to threats to privacy. Contrary to the views of Administration spokesmen it is not enough to tell agencies to gather and keep only data which is reliable by their rights for whatever they determine is their intended use, and then to pit the individual against government, armed only with a power to inspect his file, and a right to challenge it in court if he has the resources and the will to do so.

To leave the situation there is to shirk the duty of Congress to protect freedom from the incursions by the arbitrary exercise of the power of government and to provide for the fair and responsible use of that power. For this reason, the Committee deems especially vital the restrictions in section 201 which deal with what data are collected and by what means. For this reason, the establishment of the Privacy Commission is essential as an aid to enforcement and oversight.

The Committee views the standards of statutory relevance for data gathering as minimum and as paving the way for more specific guarantees in each area. The Committee rejects in part and supplements the position of the White House representative, the Chairman of the Domestic Council Committee on Right of Privacy, who testified that "the Federal Government should collect from individuals only the amount and types of information that are reasonably necessary for public protection." He stated "I do not think it is possible to develop a standard of reasonableness in any more precise way than to ask people to exercise their very best judgment and to exercise the utmost restraint in the amount of information they collect."

The Committee found many helpful definitions of privacy and confidentiality in seeking to define the concepts and principles developed in the provisions of S. 3418.

A useful statement is offered by the report on Data Banks in a Free Society project by the National Academy of Sciences, which distinguishes them in the following terms:

> *Privacy* is independent of technological safeguards; it involves the social policy issues of what information should be collected at all and how much information should be assembled in any one information system. [For purposes of the principles implemented by this bill for the Federal executive branch, the Committee reads this to include constitutional and statutory prohibitions or restraints.]
>
> *Confidentiality* is the central issue for which technological safeguards are relevant. Where an organization has promised those from whom it collects information that unauthorized uses will not be made by persons inside or outside that agency, making good that promise of confidentiality requires record security controls in both manual and computerized files.
>
> * * *

"Privacy", then, is a shorthand term for the restraint on the power of government to investigate individuals, to collect information about their personal lives and activities in society or in ways which are banned by the Constitution, or for reasons which have little or nothing to do with the purpose of government or of the agency involved, as their powers are defined by the Constitution and specific statutes.

Therefore, the Committee believes that the conclusions of study groups set up in the executive branch to study computer technology must be supplemented by the complaints from citizens and evidence gathered by numerous congressional committees on the over-reach of its information power by the Federal executive branch. This characteristic distinguishes S. 3418 from other proposals on "privacy."

State Laws

S. 3418 is further needed to complement State and municipal laws and regulations which have been adopted to protect individual privacy and confidentiality of records, and which, in some cases, provide more detailed and more effective protections than S. 3418. Governors and others have expressed concern that despite all the States may do to provide guarantees, they are not effective once the data are integrated in a Federal information system or transferred to a Federal data bank. S. 3418 will safeguard and supplement the efforts of State legislatures.

Coverage: Private, State and Local

As reported, the bill applies to Federal personal information systems, whether automated or manual, and to those of State, local and private organizations which are specifically created or substantially altered through grant, contract or agreement with Federal agencies, where the agency causes provisions of the act to be applied to such systems or files or relevant portions.

As introduced, S. 3418 applied to all governmental and private organizations which maintained a personal information system, under supervision of a strong regulatory body, with provision for delegating power to State instrumentalities.

The Committee has cut back on the bill's original coverage and ordered the Privacy Commission to make a study of State, local and private data banks and recommend precise application of the Act where needed.

The original coverage reflected the recommendations of the HEW Secretary's Committee for "enactment of its code of fair information practice for all automated personal data systems," but which noted that it would "wisely be applied to all personal data systems whether automated or manual."

Hearing witnesses and other commentators advocated nationwide application of the Act to protect individual privacy and other rights from invasion by Government and the institutions and organizations of society.

Total coverage was advocated by the representative of the American Civil Liberties Union citing examples of cases and programs to show that information collected by State, local and private institutions can be every bit as harmful to the individual. These included the reported need for additional controls over the retail credit industry, whose five largest companies maintain files on 54 million people; the Medical Information Bureau in Greenwich, Connecticut, a major source of medical information on 13 million Americans for life insurance companies; the use by the banking industry of an Electronic Funds Transfer System to centralize an individual's charges all over the community and automatically deduct them from the individual's bank account; the uncontrolled access to customer records and cancelled checks afforded by financial institutions to law enforcement officials and other investigators in the absence of subpena and notice to the individual.

Professor Miller testified in 1971 on behalf of a regulatory commission with power to embrace the activities of "non-Federal information gatherers that might adversely affect the rights we are trying to protect. The regulators should be particularly attentive to the interlocking relationships that have begun to spring up between Federal and local data handlers in the law enforcement field and the fact that many of the Nation's major corporations maintain dossiers on millions of Americans. Close scrutiny of the latter category of data banks is becoming imperative because there is growing reason to believe that these files are exchanged both within the private sector and with law enforcement and surveillance groups at all levels of government. In short, once standards are established for Federal systems I believe that it eventually will become necessary to apply them to certain non-Federal systems."

Similar findings of interlinking networks for the governmental and private sectors were found by the Academy of Sciences project.

Professor Vern Countryman, in an article submitted for the hearing record, has detailed cases, congressional hearings, and practices involving privately compiled dossiers by commercial compilers, punitive compilers, and benevolent compilers.

Reports filed for the hearing record from the Freedom of Information Center of the University of Missouri School of Journalism, describe investigative practices and intrusive data-gathering technique in the private sector.

Problems of privacy, standards, confidentiality and security in medical and health records programs were described for the subcommittee by doctors in private practice and in State government.

Extension of legislative coverage to student records procedures for gathering, disclosure, and dire process in educational records was advocated by Senator James L. Buckley and by witnesses for the Citizens Committee for Education.

Other witnesses advocated coverage of State and local systems, but not of the private sector.

Despite calls by these and other witnesses for total or partial coverage, the Committee was persuaded to delay a decision on total application by considerations of time and investigative resources for developing a full hearing record and for drafting the needed complex legislative solution for information abuses in the private sector, beyond those presently covered by the Fair Credit Reporting Act and its pending amendments.

Former Secretary of Health, Education, and Welfare Elliot Richardson noted the lack of a precise hearing record and suggested legislation "to establish authority in an existing Federal agency or in some new instrumentality established in part for that purpose, to make inquiry, hold hearings, and report to Congress if it finds a *prima facie* showing of need for legislation to assure fair information practice in some particular industry or other segment of the nongovernmental organizations of America. Congress could then take whatever action toward developing additional legislation seemed necessary."

Mr. Richardson endorsed coverage of State and local activities "substantially affected by their relationships with Federal agencies, as a consequence of (1) Federal fiscal contributions, (2) Federal record-keeping or data-collection and reporting requirements, or (3) cooperative arrangements among intergovernmental personal data system."

Dr. Westin, while endorsing coverage of intergovernmental computers systems, opposed the total coverage of the original bill, citing "the impracticality and dangers involved in trying to regulate and register many tens or hundreds of thousands of files of every kind." He recommended "an instrumentality to lead private organizations to adopt codes of fair information practice as thier voluntary policies, and proposed creating a national commission on private, interstate personal data systems." This commission should, testified Dr. Westin, "examine the conduct of those nationwide personal data systems that affect the rights, opportunities, and benefits of Americans, holding hearings as necessary and with a strong, competent staff to make on-site visits and study the real practices of organizations, not just their formal policies.

"The creation of such a commission should provide an extremely valuable force acting on the private sector. It would push privacy, confidentiality, and due process issues to the top of the organizational agenda, and into the design, testing, and operational thinking of data-system managers and their staffs. It would move the computer industry and computer professionals into high gear, as consultants to the user organizations, developers of new techniques and materials, and innovators in cost-effective responses."

Numerous representatives of private organizations and of business and industry opposed the total coverage of the bill, citing the lack of hearing record, the existing requirements of the Fair Credit Reporting Act, and prohibitive costs of implementing S. 3418 in the private sector without passing on the costs in consumer services. Most indicated support for or lack of opposition to, a commission study of privacy invasions by the private sector.

RIGHT OF ACCESS AND CHALLENGE

The Committee believes that the size of the Federal Government, the sheer number of personal records it must handle, and the growing complexities of information technology require that the full protections against abuses of the power of government to affect the privacy of the individual and the confidentiality of personal information must depend in part upon the participation of the individual in monitoring the maintenance and disclosure of his own file.

To this end, we agree with the members of numerous respected study bodies that an individual should have the right to discover if he is the subject of a government file, to be granted access to it, to be able to assure the accuracy of it, and to determine whether the file has been abused by improper disclosure.

The Committee agrees with the conclusion of one government study that "In the majority of cases, the citizen's right of access to information kept on him by the Federal Government will not interfere with the ongoing program of the agency. In addition, giving the individual a right of access often will be a desirable adjunct to any other system designed to insure file accuracy."

Furthermore, the Committee adopts the timely observation of one scholar from the Council on Science of Technology study that "giving the individual maximum ability to examine what the Government knows on the person should help promote citizen confidence in activities of the Federal Government and is essential to assure that notions of due process are employed when decisions are made on the basis of personal information."

So important does the Committee consider procedures required by the bill on this matter that it is determined that any exemptions from such provisions sought under the rule-making scheme of the bill must be kept to an absolute minimum and must not be made on the basis of parochial agency concerns. It finds support for this stand in the conclusion of the report of the HEW Secretary's Advisory Committee on Automated Personal Data Systems that:

> No exemption from or qualification of the right of data subjects to have full access to their records should be granted unless there is a clearly paramount and strongly justified societal interest in such exemption or qualification. . . . The instances in which it can be convincingly demonstrated that there is a paramount society interest in depriving an individual of access to data about himself would seem to be rare. (pp. 61, Report.)

The exemptions allowed from observance of these standards are for three purposes only, national defense and foreign policy and

certain law enforcement investigative and intelligence matters where access and challenge rights are found to damage the purpose for which the information was collected.

The Committee recognizes that while many agencies afford such rights, many agencies deny them with respect to certain files. Allowing only these narrow areas for exemption may well promote the reassessment of existing practices whereby individuals are deprived of full access to records about themselves, and some agencies, in the year before the Act takes effect, may well see fit to seek special legislation permitting special treatment of certain files they hold. Meanwhile, the Committee is persuaded by the language of the HEW report:

> Many organizations are likely to argue that it is not in the interest of their data subjects to have full access. Others may oppose full access on the grounds that it would disclose the content of confidential third-party recommendations or reveal the identity of their sources. Still others may argue that full access should not be provided because the records are the property of the organization maintaining the data system. Such objections, however, are inconsistent with the principle of mutuality necessary for fair information practice.

The relevance of the rights of access and challenge to the principle of accountability in government, to efficient achievement of management goals and to a public sense of social justice is recognized in a 1970 report made by the Project SEARCH group to the Justice Department. That report called for a citizen's right to access and challenge to certain law enforcement records, but it stated the following reasons for its conclusions which the committee finds worthy of general application:

> First, an important cause of fear and distrust of computerized data systems has been the feelings of powerlessness they provoke in many citizens. The computer has come to symbolize the unresponsiveness and insensitivity of modern life. Whatever may be thought of these reactions, it is at least clear that genuine rights of access and challenge would do much to disarm this hostility.
>
> Second, such rights promise to be the most viable of all the possible methods to guarantee the accuracy of data systems. Unlike more complex internal mechanisms, they are triggered by the most powerful and consistent of motives, individual self-interest.
>
> Finally, it should now be plain that if any future system is to win public acceptance, it must offer persuasive evidence that it is quite seriously concerned with the rights and interests of those whose lives it will record. The committee can imagine no more effective evidence than authentic rights of access and challenge.[1]

[1] Project SEARCH, Committee on Security and Privacy, Technical Report No. 2, July 1970, p. 28.

Law Enforcement Files

Title II of S. 3418 sets general standards of fair records keeping which apply to practically all government files, including those maintained by law enforcement agencies. Although various committees of the Congress [1] have been considering legislation which specifically addresses confidentiality of law enforcement files, the Committee is of the view that prospects for that legislation is sufficiently unclear so that S. 3418 should apply in its general terms to such files until such time as the law enforcement privacy legislation is enacted.

Therefore the Committee decided that, to the extent feasible, S. 3418 should apply to law enforcement files but that such application should not be inconsistent with the two major criminal justice privacy bills, introduced early this year, S. 2963 by Senator Ervin and S. 2964 by Senator Hruska on behalf of the administration. S. 3418 as amended by the Committee would apply the general standards of title II, including the general updating and accuracy requirements and provisions affording right of access to most law enforcement files.

The Committee recognizes, however, that there are two general classes of files maintained by agencies with law enforcement functions, criminal history or record files on the one hand and intelligence and investigative files on the other. The first class of information, defined for the purposes of S. 3418 as "criminal history information" includes routine records of arrests and court dispositions sometimes called rap sheets. As a general principle these records are subject to all the requirements of title II including the right of access provision. This is entirely consistent with both the Ervin and administration criminal justice privacy legislation. Indeed, Director Kelly of the FBI, in testimony before the Subcommittee on Constitutional Rights, expressed support for the general access and challenge provisions contained in the two criminal justice privacy bills and replicated in S. 3418:

> These bills provide for an individual to obtain access to his own criminal offender record, and also provide procedures for him to challenge that record. I support these provisions. Currently, the FBI provides copies of offender record information . . .

As for the other general provisions of title II, none of these provisions are inconsistent with the criminal justice privacy legislation in particular as they apply to criminal history information. Furthermore, S. 3418 permits each agency to promulgate its own regulations implementing the Act and this should provide sufficient flexibility so that the Attorney General will not undermine good law enforcement practices in promulgating regulations. Indeed, since early this year the Justice Department has been drafting regulations which address most of the basic issues raised by S. 3418. Those regulations set certain standards for the operation of any routine exchange of criminal history information by the FBI and for the funding of criminal history record systems on the State and local level by the Law Enforcement Assistance Administration. Although the Justice Department might have to

[1] The Senate Subcommittee on Constitutional Rights and House Subcommittee on Civil Rights and Constitutional Rights.

carefully review these regulations, if this legislation is passed, their scope and thrust are essentially what would be required of the Department of Justice by this legislation.

The second class of information generally maintained by law enforcement agencies are intelligence, or investigative files. These files contain highly sensitive and usually confidential information collected by law enforcement officers in anticipation of criminal activity, such as by organized crime figures, or in the course of investigating criminal activity which has already occurred. It was the Committee's judgment, shared by most criminal justice privacy experts and reflected in the pending criminal justice privacy legislation, that all of the provisions of title II of S. 3418 could not be applied to such sensitive information. In particular, it would not be appropriate to allow individuals to see their own intelligence or investigative files. Therefore, the bill exempts such information from access and challenge requirements of title II. However, most of the other general accuracy and updating provisions would apply, subject, of course, to the rules and regulations issued by the agency head in the course of implementing such provisions.

Obviously, these general provisions on law enforcement records are not entirely adequate. The two criminal justice privacy bills address this subject in considerable detail and are the result of at least two years of careful study and revision by the Subcommittee on Constitutional Rights and the Justice Department. However, the Committee feels that general privacy legislation must assure subjects of law enforcement files at least these minimal rights until such time as the more comprehensive criminal justice legislation is passed.

Privacy Protection Commission

It is clear that many of the information abuses over the last decade could have been avoided with the help of an independent body of experts charged with protecting individual privacy as a value in government and society.

Commentators on privacy for years have also cited the need for such an agency to help deal in a systematic fashion with the great range of administrative and technological problems throughout the many agencies of the Federal Government.

Title I of S. 3418, as amended, establishes a Privacy Protection Commission composed of five experts in law, social science, computer technology, and civil liberties, business, and State and local government and supported by a professional staff. The Commission would be empowered to:

> Monitor and inspect Federal systems and data banks containing information about individuals;
>
> Compile and publish an annual U.S. Information Directory so that citizens and Members of Congress will have an accurate source of up-to-date information about the personal data-handling practices of Federal agencies and the rights, if any, of citizens to challenge their contents;
>
> Develop model guidelines for implementation of this act and assist agencies and industries in the voluntary development of fair information practices;

Investigate and hold hearings on violations of the Act, and recommend corrective action to the agencies, Congress, the President, the General Accounting Office, and the Office of Management and Budget;

Investigate and hold hearings on proposals by Federal agencies to create new personal information systems or modify existing systems for the purpose of assisting the agencies, Congress, and the President in their effort to assure that the values of privacy, confidentiality, and due process are adequately safeguarded; and

Make a study of the state of the law governing privacy-invading practices in private data banks and in State and local and multistate data systems.

Need for a Privacy Protection Unit

There is an urgent need for a permanent staff of experts within the Federal Government to inform Congress and the public of the data-handling practices of major governmental and private personal information systems. As a recent study by the Judiciary Subcommittee on Constitutional Rights graphically demonstrates, there has been a proliferation of Federal information systems and data banks which, if misused, can do irreparable harm to the privacy and economic well-being of millions of persons. "Data Banks and a Free Society," the study done for the National Academy of Sciences by Professors Alan F. Westin and Michael A. Baker, similarly demonstrates such harm inherent in large personal information systems maintained at all levels of government and by private industry.

Although recent attempts to turn Federal tax records into weapons of political and personal revenge have come to light, along with many other record abuses, the major threat to most Americans lies in the inadvertent, careless, and unthinking collection, distribution, and storage of records which may be inaccurate, incomplete, or irrelevant to legitimate governmental needs. This threat has grown tremendously as developments in telecommunications, photocopying, and computer technology have accelerated and with expanded data-swapping among government agencies and throughout private industry.

It is now clear that Congress, with its limited technical staff and multitude of functions, cannot keep track of these developments in every Federal agency and for every data bank with the depth of detail required for consistently constructive policy analysis. The Constitutional Rights Subcommittee data bank study and other agency-by-agency studies have each taken years to complete, and have documented the frustrations of agency delays, withholding of data, and camouflage of governmental activities. Citizens also have no place to turn to find out which agencies or companies maintain, distribute, and use personal information about them. Agencies and businesses would similarly benefit from the existence of an authoritative source of information about their record-keeping practices which would protect them from misinformed and inflamatory criticism.

In addition, there is an urgent need for a staff of experts somewhere in government which is sensitive both to the privacy interests of citizens and the informational needs of government and which can furnish expert assistance to both the legislative and executive branches.

In recent years, controversies over privacy and government data banks have arisen after executive branch decisions have been made. The Commission will serve the important purposes of raising and resolving privacy questions before government plans are put in operation. Agencies need help to incorporate newly-refined concepts of individual liberty into their current procedures without unnecessary disruption and confusion. Congress and the President need help in identifying those areas in which privacy safeguards are most urgently needed and in drafting legislation specifically tailored to those problem areas.

There are now over 100 privacy bills before Congress. Most are of unquestionable merit, but only a few can receive the kind of sustained attention to survive the legislative gauntlet. The proposed Commission would help Congress deal with those bills in two ways. First, it would obviate the necessity of enacting many of them into law by inducing agencies and industries to adopt their own fair information practices. Second, the Commission would help Congress and the President by narrowing down the range of legislative options and drafting bills designed to achieve a good "fit" between privacy values and other values in the context of often unique data-keeping activities.

It may well be that regulatory functions will eventually have to be added to the Commission's powers in order to assure that privacy, confidentiality, and due process become an integral part of governmental and private data systems. However, the Committee has decided not to address this area in the legislation pending the Commission's study.

The original version of S. 3418 would have created a Federal policy board with regulatory powers to investigate and issue cease and desist orders for violations of the Act. The Committee believes that it does not have sufficient evidence to support a case for vesting broad regulatory powers in a board charged with administrating the Act. Rather, a much more effective and less cumbersome procedure will permit an individual to seek enforcement of his rights under procedures established by each Federal agency. Ultimate enforcement of those rights and challenges to agency judgments would rest with United States District Courts. By taking this action, the Committee did not mean to preclude a future decision by the Congress to vest regulatory functions in the Commission to assure that privacy, confidentiality, and due process become an integral part of governmental and private data systems.

Public administration and privacy experts have urged a cautious approach to regulation on two grounds. First, there is much more that privacy advocates need to know about information systems before they are in a position to make demonstrably constructive regulatory policy proposals. Second, there is substantial evidence that agencies and companies are not inherently hostile to letting individuals have more of a say in what the files say about them, provided that the changes can be made in an orderly, efficient, and economically sound manner. The work of the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Data Systems, Vice President Ford's Domestic Council Committee on the Right of Privacy, and the National Academy of Sciences Project on Computer Data Banks, clearly demonstrate that the right of privacy has its advocates within the executive branch. Testimony before the Committee by

State officials was nearly unanimous in citing a need for higher standards and better regulation of privacy practices in their jurisdictions. Statements by private industry representatives have persuaded the Committee that a substantial measure of industry cooperation can be anticipated.

Thus, the Committee believes that it would be a mistake for the Privacy Protection Commission to begin its work in an adversarial posture, either as a regulatory or ombudsman-type agency. Those roles may come in time, but they should be the product of specific legislation and come only after efforts to achieve voluntary reforms have failed. Meanwhile, awareness that the Commission might be vested by Congress with regulatory powers at some future time should have a salutory effect on those agencies which may be tempted to ignore its suggestions, or which fail to give its model guidelines the deference due them.

Locating the Privacy Unit

The Committee has concluded that the best place to vest these new functions would be in an independent commission. The decision was arrived at with some reluctance, because members of the Committee share the unwillingness of many Members of Congress to create still more independent commissions. On balance, however, the commission route seemed the best solution for the abuses and potential threats which have been documented.

Having concluded that an expert staff and an independent body was needed somewhere in the Federal Government to supply information and advice and conduct investigations, the Committee considered three alternatives, as described in testimony before Committee by Dr. Christopher H. Pyle. The first was to place the unit in the General Accounting Office, modeled on the Office of Federal Elections. The second was to locate it in the Office of Management and Budget, much like the Statistical Policy Division which polices Federal questionnaires. The third alternative was to create an independent commission.

The Committee chose not to recommend vesting the investigatory and advisory functions in the GAO because it would be unwise to dilute the GAO's important auditing function with this kind of substantive policy assignment. Except in rare instances, responsibility within Congress for policy development should rest with its committees. Also, placing the investigative role in the GAO might limit the unit's ability to study multi-state and commercial information systems not dependent upon the Federal budget, which is the focus of the GAO's attention.

Similar considerations persuaded the Committee that the unit could not achieve its full potential as part of the Office of Management and Budget. Moreover, the Committee was of the opinion that the privacy protection unit should be available to congressional committees as well as executive agencies—a relationship which could not be guaranteed by making it part of the President's staff. On the other hand, by creating the unit as a commission, its reports and expertise could be available to both the GAO and OMB.

The Committee received suggestions that creation of such an independent commission should be delayed in order to develop legislation charging it with the functions of dealing with classification and freedom of information issues, as well as privacy and civil liberties.

While they pose significant problems, these other two subject areas go to different considerations of government. Creation of a privacy commission is recognition of the fact that the Congress intends to afford access to the decision-making centers of government to interests which promote the privacy of individual Americans against overly-intrusive or arbitrary government information policies. To dilute the quality of that access, as institutionalized in the structure by the Privacy Commission, would defeat the purpose of the legislation. It would reduce the viability of privacy as a matter of concern in the Federal Government. By thus denying itself the full strength of the investigative help needed to protect privacy and due process in the years ahead, Congress would dilute, in turn, the quality of protections which it and the other branches of Government might otherwise afford to those amendments in the Bill of Rights which safeguard privacy.

The administration has opposed the creation of a commission partly for reasons of cost. It is the Committee's belief, however, that the Commission is vitally needed to promote the quality of legislative and administrative oversight which will provide a privacy bulwark for Americans in the years ahead. It is expected, furthermore, that the savings it will effect in the Federal Government will far outweigh the immediate cost.

Enforcement

The Act is enforceable in the courts with the aid of Congress and the Privacy Commission.

As Elliot Richardson, former Secretary of three executive branch Departments, informed the Committee:

> The requirements of fair information practice are so much in the interest of organizations, as well as of the individuals about whom records are maintained, that there should be little difficulty in agencies adhering to them and little occasion for court enforcement suits. Enforcement provisions are needed, however, to create a strong and reliable incentive to overcome the initial bureaucratic resistance to change that might otherwise prove to be a crucial obstacle to the prompt and full achievement of fair information practice. Frivolous suits, no doubt a matter of concern to some, would be promptly subject to motions for summary dismissal.

Except for the act of keeping secret data banks and improper disclosure by Commission employees, there are no criminal penalties in the Act. As introduced, the original bill contained strong criminal penalties for employees and others who violated or contributed to the violation of the Act. These penalties were deleted in Committee for two main reasons: the difficulties of effective enforcement through such criminal prosecutions and the possibility that the threat of prosecution may preclude that "Whistleblowing" and disclosure of wrongdoing to

Congress and the press which helps to promote "open government."

Instead, the mandates of S. 3418 are enforceable through the civil challenges of the Attorney General or of private citizens with real or suspected grievances or claims of violations of the Act. Given the difficulties of time and resources, private enforcement through litigation is not likely to affect more than glaring violations of the Act. Much will depend on the zeal and the good faith of the Attorney General and the President in enforcing the terms of the new law.

As always, the press and communications media will contribute to the enforcement of the Act through its investigation and exposure of wrongdoing, a function eased by the requirements in S. 3418 that decisions be made on the open record by responsible officials and that precise notices be published containing the details of government policy where it affects personal privacy.

Administratively, the agencies may be called to account by Congress and the President through the monitoring and investigative activities of the Privacy Commission and its reporting of violations.

Despite these guarantees, the Committee acknowledges there is no way that the Congress, the press, or the public can assure strict administrative observance of the exercise of the power of the Federal Government pursuant to the standards of the Act. There will no doubt be some diversity of views as to what constitutes compliance within particular agencies.

Realistically, therefore, the implementation of the Act rests, finally, with the departments and agencies of the executive branch and the good faith, ethical conduct and integrity of the Federal employees who serve in them.

SOCIAL SECURITY NUMBER AND IDENTIFIERS

As introduced, S. 3418 made it unlawful for any person to require an individual to disclose or furnish his Social Security account number for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual because of refusal to disclose or furnish the number, unless the disclosure or furnishing of the number was specifically required by Federal law.

The Committee considers this usage of the number of a government file one of the most serious manifestations of privacy concerns in the Nation. However, it received conflicting evidence about the effects of this section, particularly the inordinate costs to the Federal Government and private businesses of changing to another identifier and reprogramming computers or reindexing files.

In view of the lack of ready independent data about the probable costs and effects of such a prohibition and in view of stricter limitations on transfer of and access to government files, the section was deleted in Committee by an 8 to 1 vote. At the same time, the issue was designated as a priority issue for study by the Privacy Commission and for report to Congress of specific legislative recommendations to meet the serious public concerns reflected in the original bill. In subsection 106(b)(1)(C), the Commission is required to examine and analyze "the use of license plate numbers, Social Security numbers,

63-619 O - 76 - 13

universal identifiers, and other symbols to identify individuals in data banks and to access, integrate or centralize information systems and files."

The Committee realizes that the number is a major element in the national debate over privacy since a common numerical identifier or symbol to designate and index each person is an essential feature of a national data bank, or indeed, of any information system which allows creation of an instant dossier or which permits quick retrieval of all personal information which flows through that system about an individual.

In recent years the Social Security number has been the identifier most used in common by government agencies and private organizations to improve efficiency of services, aid management functions, prevent fraud and reduce errors in identification of people.

Citizens' complaints to Congress and the findings of several expert study groups have illustrated a common belief that a threat to individual privacy and confidentiality of information is posed by such practices. The concern goes both to the development of one common number to label a person throughout society and to the fact that the symbol most in demand is the Social Security number, the key to one government dossier.

Of major concern is the possibility that the number may become a means of violating civil liberties by easing the way for intelligence and surveillance uses of the number for indexing or locating the person.

In this connection, a Constitutional Rights Subcommittee report on the intelligence-gathering by the military from its own agents and the files of other Government agencies, shows that individuals were often indexed in the Army computers by their Social Security numbers. Complaints to the Constitutional Rights Subcommittee also showed that government pressures people to disclose their Social Security number on administrative, statistical, and research questionnaires of all kinds, including income tax forms, HEW questionnaires asking whether elderly people buy newspapers and wear false teeth, and many others.

Every serviceman is now identified by his Social Security number, a development of intense concern to some groups who were not able to persuade congressional committees or the Pentagon to reverse the course.

A cross-section of such complaints appearing in the subcommittee hearings shows that people are pressured in the private sector to surrender their numbers in order to get telephones, to check out books in university libraries, to get checks cashed, to vote, to obtain drivers' licenses, to be considered for bank loans, and many other benefits, rights or privileges.

In many cases in the private sector, he is informed that the number is necessary for identification purposes, yet on its face, the Social Security card states that it is *not* to be used for identification purposes. This proviso was initially included in the Social Security program to prevent reliance on the card for identification because a person could acquire several of them under several identities and there frequently was no agency investigation of the information provided in order to obtain a number.

A list of the Federal Government's uses of the number, authorizations, and the texts of applicable statutes, Executive order, and regulations appears in the appendix of the hearings together with excerpts of Government reports on this subject.

The HEW Secretary's committee found that "the Federal Government itself has been in the forefront of expanding the use of the number, that its actions have actively promoted the tendency to depend more and more upon the number as an identifier—of workers, taxpayers, automobile drivers, students, welfare beneficiaries, civil servants, servicemen, veterans, pensioners, and so on." It concluded: "If use of the SSN as an identifier continues to expand, the incentives to link records and to broaden access to them are likely to increase. Until safeguards such as we have recommended . . . have been implemented, and demonstrated to be effective, there can be no assurance that the consequences for individuals of such linking and accessibility will be benign. At best, individuals may be frustrated and annoyed by unwarranted exchanges of information about them. At worst, they may be threatened with denial of status and benefits without due process, since at the present time record linking and access are, in the main, accomplished without any provision for the data subject to protest, interfere, correct, comment, and in most instances, even to know what linking of which records is taking place for what purposes."

While specific laws mandate or have been interpreted to permit the use of the number in a few Federal programs, most agencies have proceeded to use it by regulation or directive. Executive Order 9397 of 1943 found it "desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single unduplicated numerical identification system of accounts", and ordered that "any Federal department, establishment or agency shall, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize exclusively the Social Security account numbers."

While some have cited this order as authority for the Federal usage, the HEW report found otherwise, noting, "It has been suggested that Executive Order 9397 was intended to apply only to instances when Federal agencies seek to number records, such as employment, attendance, performance, or medical records. . . . To interpret the order as applying to all kinds of Federal agency record systems is arguably beyond the meaning of its language. In any case, it appears that Federal agencies are free to use the SSN in any way they wish, and no instance has come to our attention in which the order has been invoked to compel or limit an agency's use of the SSN." (p. 117)

The HEW Secretary's committee came to the following conclusions about the need for legislation on this matter: "If the SSN is to be stopped from becoming a de facto Standard Universal Identifier, the individual must have the option not to disclose his number unless required to do so by the Federal Government for legitimate Federal program purposes, and there must be legal authority for his refusal. Since existing law offers no such clear authority, we recommend specific, preemptive, Federal legislation providing that the individual has the right to refuse to disclose his SSN to any person or organiza-

tion that does not have specific authority provided by Federal statute to request it . . . and the right to redress if his lawful refusal to disclose his SSN results in the denial of a benefit."

The report contained other recommendations about the need for constraints on the use of the number and on its dissemination, and it cited the need for congressional review of all present Federal requirements for use of the number to determine whether they should be continued, repealed, or modified.

The Committee expects the Privacy Commission study to undertake such a study for the public and private sector.

A number of departments and agencies opposed the provision in S. 3418 limiting the use of the Social Security number. These included the Commerce Department, Civil Service Commission, Defense Department and the Securities and Exchange Commission. All cited the need for use of the number as an identifier to achieve administrative ends, and the inordinate and prohibitive costs of reprogramming with an alternative number. Numerous private business, banks and industries uniformly opposed this section.

Computer and data professionals from State and local government also opposed the provision, testifying that such prohibitions on its use "would impose a tremendous financial burden on the States and an alternate identifier would have to be developed."

Mailing Lists

The bill now prohibits Federal agencies from selling or renting mailing lists except as authorized by law, but does not require names and addresses to be kept confidential, thus allowing inspection where these are public records. It requires private organizations maintaining a mailing list to remove the individual's name upon request.

A major avenue by which personal privacy and confidentiality may be invaded is the practice of the Federal Government of selling and renting names, addresses and personal data in their files for use in commercial and other mailing lists. Such practices may cause a violation of the tacit or formal agreement by which the agency collected or acquired the information for its own authorized purposes. Laws promoting open records in government have resulted or may result in administrative contracts on agreements to sell the data in bulk, either as a convenience to commercial or other users, or to publicize and promote the purposes of the agency.

While a few examples might be found in which the sale or rental of mailing lists by Federal agencies without specific statutory authority serves a useful purpose, the Committee concludes for several reasons that such action is totally inconsistent with the purposes of the bill as amended. One of these purposes is to entitle an individual to a large measure of control over who, outside of a Federal agency maintaining information about him, has access to his personal information. Mailing lists constitute such personal information when, for example, they represent a group of individuals possessing a certain set of characteristics. The disclosure of this personal information can be damaging to the individual. Therefore, section 206(a) of the bill, as amended, prohibits the sale or rental of lists of names and addresses by Federal agencies unless the sale or rental is specifically authorized by law.

Legislation on this subject has been offered for a number of years. These problems are addressed in S. 3116, introduced by Senator Hatfield and pending before the Constitutional Rights Subcommittee.

Senator Hatfield stated "the real thrust of S. 3116 is not what is received in one's mailbox but privacy and the question of individuals' right to control what is known about them."

He cited the stockpiling of personal information in the businesses who compile and sell lists and other data for commercial purposes. Primarily, this means selling or renting lists to the direct mail industry.

The Committee was told that "lists for this industry are compiled from every imaginable source—telephone, books, magazine subscription lists, credit card lists, church rosters, club memberships, government agencies, newspaper, announcement of birth, death, graduation and from seemingly, inviolate sources such as doctors, dentists, and schools. This flourishing business exists largely without the knowledge of the people who are providing the profit, the people whose names and personal data keep this wheel turning."

Testimony from the Direct Mail Marketing Association shows that it is their recommended practice to remove a person's name from their list if requested to do so. However, only some people know about this service, and the distribution of information through lists is so widespread that people who do manage to get off lists through such a service, have no way of controlling what all the other companies do.

The bill now requires no more of the private sector than that an organization engaged in business in interstate commerce shall remove the individual's name from a mailing list, upon request. Where lists are maintained by private companies, the Committee believes that the decision as to who should be allowed to rent or buy them is a decision best left up to each individual business. However, where such lists are maintained by government agencies, or where names and addresses are sold or rented, the Committee firmly believes that the decision must not be left to individual agency administrators.

Subsection 206(b) requires all persons or organizations engaged in interstate commerce to comply with the written request of an individual who wishes to have his name and address removed from their lists that are used for direct mail solicitation.

This provision represents a sound business practice which is followed by many of the largest and most respectable direct mailers in the country. The Direct Mail Marketing Association, which represents several thousand users of direct mail marketing and advertising in America, has stated in writing to the Senate Government Operations Committee that its Mail Preference Service is specifically designed to permit an individual to have his name removed from its members' lists upon request.

The Committee has been advised by representatives of the Direct Mail Marketing Association and by numerous prominent direct mailers that this practice creates more profitable lists by allowing for the removal of names of individuals who are unlikely to purchase goods or services from the soliciting organization.

The purpose of this provision is to extend this practice to all organizations and to expand the protection to all individuals. It is consistent with the best practice in American industry and with the programs and standards of the Association representing those companies with direct interest in this problem.

The Committee believes such a requirement is a simple and fair one which will not necessitate a revision of private business procedures. Mail order businesses may continue to compile mailing lists and solicit through the mail. The widespread sentiment on this subject for action was noted by Congressman Frank Horton, sponsor of House bill, H.R. 3995, who reported 65 House members sponsoring the bill, 34 Republicans and 31 Democrats.

A survey of mailing list practices of Federal departments and agencies made by the Congressman and another by the House Government Operations Subcommittee chaired by Congressman Moorhead, were offered by Congressman Horton for the hearing record.

The threat to individual privacy from the selling and renting of names and personal information from government files and the use of mailing lists by the mailing list industry was found to be an appropriate subject for privacy legislation by the National Academy of Sciences Project Report. The Committee agrees with the report that the standard of the Direct Mail Marketing Association, mere removal of one's name, is not enough for Government agencies. As the Academy report states, "For many people, this does not resolve the basic privacy issue: when individuals give information about themselves to government agencies for one purpose, usually under legal compulsion to report, should their names, addresses, and data about their occupations, ownership, military service, or other activities be made available to organizations that would use the information for purposes that these individuals consider intrusive?

"In time of major problems of housing, education, crime, race relations, pollution, and peace, it may seem a disturbingly trivial matter to worry about government records leading to the receipt of mail advertisements that some individuals do not want. But the issue symbolizes something we cannot afford to ignore—how do we make the individual's informed consent a more respected and controlling feature in organizational society? Our approach to this problem should not be to make matters confidential which have long been considered open for public access; rather, it should be to find a way to accommodate those who feel their privacy is intruded upon by such direct mail practices. (Report, p. 385)"

Section-by-Section Analysis

TITLE I—PRIVACY PROTECTION COMMISSION

Section 101

ESTABLISHMENT OF COMMISSION

Title I establishes a Federal Privacy Commission, an independent body which the Committee deems absolutely essential to aid in the administrative and enforcement of the act, and to conduct a study of other private and governmental information systems.

Section 101 provides that the five full-time members of the Commission would be appointed by the President subject to confirmation by the Senate. In order to assure the kind of expertise necessary for dealing with the legal, political, social and technological aspects, a commissioner should be considered for selection in part by reason of

his knowledge in one or several of the areas of civil rights and liberties, law, social sciences, computer technology, business, and State and local government. Not more than three of the members of the Commission shall be from the same political party. Commissioners shall serve for terms of three years and for no more than two terms. The President shall select the Chairman of the Commission from its members and he shall be the official spokesman of the Commission in its relations with Congress, the Federal Government and the general public. In this capacity, the Chairman would be expressing the view of the entire Commission. Of course, this would not prevent any other Commissioner from speaking his views, testifying, or providing information to Congress, the Executive or the public. In all other respects, the Chairman shall have equal responsibility and authority in all decisions and actions of the Commission with other members and each member shall have one vote on the Commission.

Section 102

PERSONNEL OF THE COMMISSION

Section 102 authorizes the Commission to appoint an Executive Director and other officers and employees and prescribe their functions and duties. The Executive Director will be compensated at a rate not in excess of the maximum for a GS–18 Federal employee.

In addition to its own employees, the Commission may contract for the services of experts and consultants to carry out its responsibilities. Where these are technicians charged with the inspection of physical and technical security of arrangements, computer equipment and systems, they should be bonded in cases where this is found appropriate.

Section 103

FUNCTIONS OF THE COMMISSION

One of the principal reasons for establishing a Privacy Protection Commission was to fill the present vacuum in the administrative process for overseeing establishment of governmental data banks and personal information systems and examining invasions of individual privacy.

Subsection 103(a)(1). Requires the Commission to publish, and supplement annually, a United States Directory of Information Systems. Each agency is required under subsection 201(c) to notify the Commission of the existence and character of each existing system or file which it maintains on individuals, or any significant expansion or modification of the system. The Commission is directed to publish this information in the Directory of Information Systems together with a listing of all statutes which require the collection of such information by a Federal agency. This is to carry out one of the fundamental principles of the Act that the existence of Federal personal record-keeping systems should not be kept secret from the Congress, the press, or the public. In particular, it is designed to give the citizen one set of accessible documents and one central location where one may reasonably be expected to find out just what agencies are likely to have a file on one and what they are likely to have done with it.

It also provides a published standard for testing and evaluating Federal collection, use and disclosure of personal information in the hands of government. The Committee considers this requirement a substitute for the original requirement of notice to everyone on whom any Federal agency maintains a file, a notice ideally designed to promote the concept of substantive due process throughout government. However, consideration of testimony from experts and of agency objections concerning costs and administrative feasibility of such a requirement resulted in its deletion and replacement by the function of the Commission in this section.

Subsection 103(a)(2). Authorizes the Commissioners to investigate and hold hearings on reports received of violations of the Act. No adjudicatory powers are vested with the Commission and enforcement of the Act rests with the Federal courts. If the Commissioners determine that a violation has occurred, they may report that violation to the President, to the Attorney General, to the Congress, to the General Services Administration where the duties of that agency are involved, and to the Comptroller General if it deems it appropriate for any auditing functions of that agency. S. 3418, as originally introduced, would have given the Commission the power to issue cease and desist orders to stop violations of the Act. The Committee decided, however, to provide for general enforcement of the Act's safeguards, and for the implementation of the exemption provisions, through the administrative channels of each agency, with ultimate review of any challenges in a United States District Court.

Subsection 103(a)(3). Model Guidelines. The Commission has not been given the power to issue rules and regulations that would b binding on other Federal agencies. However, it is directed to develop model guidelines for implementing the provisions of the Act with interagency consultation and the assistance of appropriate experts in special subject areas. The Committee would expect that other Federal agencies would look to these guidelines before adopting their own rules and their procedures by which individuals could exercise their rights under this legislation.

The Commission is further directed to assist Federal agencies in preparing regulations to meet the technical and administrative requirements of this Act. It is expected that the Commission will retain or contract for expert assistance in information management and technology and other fields in order to provide resources that may not be available to each agency.

Subsection 103(b). Requires the Commission to review, and report on proposed data banks and substantial alteration of existing ones. For this reason, subsection 201(g) requires that Federal agencies report to the Commission on proposals to establish data banks and personal information systems, to significantly expand existing data banks and information systems, to integrate files or establish programs for records linkage within or among agencies, or to centralize resources and facilities for data processing.

The review anticipated here is for several purposes. The Commission is directed to review these reports in order to assess the potential impact of any such proposal on the privacy, due process, and other personal or property rights of individuals or on the confidentiality of personal information. This would include the physical,

technical and administrative security of the data bank or computerized information system. The Committee acknowledges that there are many definitions of privacy and that there is no one precise definition as it relates to the exercise by an individual of rights guaranteed to him under the Constitution or of his right to own and possess property. Each amendment to the Constitution carries with it guarantees against governmental invasions of a particular aspect of individual privacy. Until the concept of privacy can be defined with more precision, the Committee believes that there is a need to study any threatened invasion of a broad range of individual rights by Federal information activities or practices.

In testimony before the Committee on Government Operations and before other committees of the Senate, questions have been raised about the impact of Federal information systems on State programs and powers as well as on the separation of powers existing between the judicial, executive and legislative branches of the Federal Government. Any proposal to establish or alter an information system should be examined in light of its potential to affect the Federal system: to take power or responsibility from the States or to grant responsibilities which should properly be carried out by a Federal agency.

Similarly, any major proposal to expand or create new information-handling technology by Federal agencies for personal data should pose questions for the Commission to attempt to answer regarding the ability of the three branches of government to discharge their responsibilities under such a new system. It is for all of these reasons that agencies must describe in their notices the following matters, under subsection 201(g):

> (1) the effects of such proposals on the rights, benefits, and privileges of the individuals on whom personal information is maintained;
>
> (2) the software and hardware features which would be required to protect security of the system or file and confidentiality of information;
>
> (3) the steps taken by the agency to acquire such features in their systems, including description of consultations with representatives of the National Bureau of Standards and other computer experts; and
>
> (4) a description of changes in existing interagency or intergovernmental relationships in matters involving the collection, processing, sharing, exchange, and dissemination of personal information.

Based upon its review of these proposals, the Commission should submit any findings and recommendations regarding the need for new legislation or administrative action to control or regulate new information-gathering techniques and technology to the President, the Congress, and the General Services Administration.

Subsection 103(c). The Commission is directed to report to the Congress the failure of any proposed data bank or information system to comply with the purposes, standards and safeguards of the Act. In most cases, a review by the Commission of proposals to establish or expand information systems should take no longer than sixty (60) days and should afford the agency sufficient opportunity to alter its proposal if a question regarding compliance with this Act is raised.

This estimate of time is predicated on the full and prompt disclosure to the Commission of agency proposals sufficiently in advance of a final policy decision by the agency to proceed with the proposal to permit adequate review by the Commission. If it is necessary for the Commission to report a failure to comply with the Act, the agency proposing an information system change shall not proceed with this proposal until sixty (60) days after receiving that notification. This is to afford the Congress and responsible executive branch officials an opportunity to act on the agency proposal. If the Commission does not make a determination that the Act has not been violated by an agency proposal, this should not constitute an endorsement of or approval of any invasion of privacy which might result from the implementation of the newer alternate information system.

In carrying out its functions under the Act, the Commission is encouraged to consult to the fullest extent practicable the heads of departments, agencies and instrumentalities of the Federal Government, of State and local governments and of private businesses and other organizations which may be affected by S. 3418. In order to carry out the duties assigned by the Congress, the Commission must be provided access and the opportunity to personally inspect a wide range of confidential material, information maintained by public agencies and private organizations and businesses. In performing its functions the Commission has the difficult task of balancing its need for information with the rights of privacy of citizens. It may, for example, be necessary for it to examine the actual contents and use of certain files held by agencies. Obviously, the Commission itself is bound by the requirements of the Act, including civil and criminal liability for any improper use or divulgence of information it receives in carrying out its responsibilities. The Committee expects the Commission to perform its tasks comprehensively, but has guarded against the creation of an Information Czar. The Commission is not intended to maintain its own files on individuals, or to retain any such personal information in its own possession. The Committee regards this legislation as a means to guard against the integration of separate files on citizens into complete dossiers. The Commission's powers should not be used to frustrate this purpose. In addition, there is no intent to require a national depository for the technical and commercial, and trade documents, or the programming secrets of government organizations and the private sector.

Subsection 103 (d)(1). Mutual cooperation will be important to the successful completion of the study of information systems and the implementation of the safeguards by the agencies covered by the Act. With regard to the Federal Government, the Commission may wish to form an interagency council to work to implement the provisions of the Act.

It is expected that the Commission will also serve as a clearinghouse for various Federal agencies and others to share information on methods of dealing with problems in administering the Act as well as assisting in the exchange of administrative and technological material related to handling of personal information.

Subsection 103(d)(2). It is probable that the Commission will need to study and initiate research projects to determine the best procedures for agency implementation and enforcement of this Act. Because of the highly technical nature of information in system management, re-

search efforts may also be directed toward developing procedures for guarding against unauthorized access to information systems and procedures for implementing the standards and safeguards provided by title to this Act. Where these have already been undertaken by the National Bureau of Standards and other Federal offices, the Commission should take appropriate advantage of those resources to prevent duplication of efforts and to aid in the coordination of Federal efforts in this area.

Subsection 103(d)(3). The Committee added to the functions of the Commission the duty to determine, in connection with its research activities, what specific categories of information should be prohibited by statute from collection by Federal agencies on the basis that the collection of such information would violate an individual's right of privacy.

Section 104

CONFIDENTIALITY OF INFORMATION

In order to fulfill its obligations properly under this Act, the Commission must have access to all data, reports, and other information requested of any department, agency or instrumentality of the executive branch as well as of any independent agency.

Since this will require access to classified documents and other highly sensitive personal information, the Commission may accept identifiable personal data only if it is necessary to carry out its powers and functions. It is directed to establish safeguards to insure that the confidentiality of the information is maintained and upon completion of the purpose for which the information is required it must be destroyed or returned to the agency or person from whom it was received. Because of the strict penalties provided for the unauthorized disclosure of information entrusted to its care, the Committee believes it would be appropriate for the Commission to assure that its technicians and any other employees are bonded before they are permitted access to sensitive information. In addition Commission employees or contractors should be extended the same privileges and be subject to the same requirements for security clearances under the Federal Security Clearance as employees of the agency who have access to the information in question. Under no circumstances should the Commission or its employees be used by another agency for unlawfully obtaining information to which that agency would not be otherwise entitled. The internal rules and regulations of the operation of the Commission should reflect the need for careful handling of this information.

Section 105

POWERS OF THE COMMISSION

The Committee is determined that the Privacy Protection Commission must have certain powers to fully implement a study of personal information systems and to conduct oversight of the proper implementation of the Act in the Federal Government.

In order to investigate reported violations of the Act, the Commission may find it necessary to hold hearings and take testimony as well as receive evidence related to such violations before making any report to the Congress or to the Attorney General. In order to obtain

sufficient information for these hearings or to assemble material for the study of information systems, the Commission is authorized to require by subpoena the attendance of witnesses and the production of books, records, papers, correspondence and documents as it deems advisable.

It is hoped that the Commission would be able to work out voluntary agreements with both public agencies and private organizations for obtaining any material necessary to carry out its statutory responsibilities. Should efforts at voluntary cooperation fail, however, the Committee believes that the role of the Commission is important enough to merit the force of law behind its requests. Under any circumstances, however, no subpoena shall be issued without a vote of the majority of the Commission. The Commission shall appear in court in its own name to enforce subpoenas issued pursuant to this Act, and it shall be represented by attorneys of its own choosing.

Testimony presented before this and other committees, as well as in noncongressional studies, has shown the need and value of the on-site inspection to ensure that regulations adopted pursuant to the Act are in fact adhered to by agencies in their normal day-to-day operations. By giving the Commission the power to take such other actions as may be necessary to implement the Act, the Committee has adopted this recommendation.

While criminal penalties for the violation of this Act are limited to the failure by an officer or employee of a Federal agency to disclose the existence of an information system or the unauthorized disclosure of certain sensitive personal information by a member or employee of the Commission, the Committee felt it was necessary to provide immunity from punishment under this Act pursuant to the provisions of Section 6001(1) of Title 18 of the U.S. Code. This "whistle-blowing section" would permit the Commission to recommend to the Attorney General that a person not be prosecuted under this Act. And this section is designed to encourage the reporting of violations in order to further strengthen the reporting of violations in order to further strengthen the oversight responsibility of the Commission.

The section would authorize the Commission to adopt interpretative rules for the implementation of the rights, standards and safeguards provided by this Act. This is to assure that the rulemaking authority of the Commission is limited to the promulgation of rules and regulations governing its own operations, organization and personnel. This section was included to insure that the courts would not interpret these model guidelines or other rules which the Commission is authorized to issue as having the force of law with respect to any other Federal agency. Rather, such guidelines shall offer only the Commission's best judgment regarding the possible implementation of its safeguards under the Act, and shall serve as a reference only for other Federal agencies to consider in adopting their own rules and regulations.

Section 106

COMMISSION STUDY OF OTHER GOVERNMENTAL AND PRIVATE ORGANIZATION

Section 106 requires the Privacy Commission to make and report on a study of the data banks, automated data processing programs, and information systems of the private sector as well as of regional and

other governmental agencies. As discussed in this report, the decision to authorize such a study is based on the Committee deferral at this time of legislation for abuses of privacy, due process, and confidentiality in the private sector, a need particularly urgent with the growth of national data banks, application of computer technology, and use of new information management practices.

The lack of adequate empirical and legal research to support needed legislation is expected to be remedied by the Commission study and its specific recommendations as to application of the principles or guarantees of this legislation to particular sectors or subject areas, or to particular information linkages between private, State, and Federal data systems. It is further authorized to make such other legislative recommendations as it may determine necessary to protect individual privacy while meeting the legitimate needs of government and society for information. Such study may, on the basis of the Commission's research, take into account the testimony on the original bill advocating regulatory oversight by the Commission or some other Federal agency of all major data banks and information systems affecting privacy.

The Committee found a particular need for examination of the laws and practices governing the kinds of information held by private information collectors which the Federal Government obtains by various means. This includes bank, health, educational, and employment records. It was partly for this reason that the Committee adopted an amendment authorizing the Commission to study what personal information the Federal Government should collect. Congressional studies revealed that most departments and agencies had little cogent knowledge on the extent of their data collection from the private sector and how their demands or their grants, contracts or agreements ultimately affected the privacy of the individual.

Despite some efforts by government and private bodies to study certain aspects of public and private information practices and computer technology, no Federal body has yet been given a broad mandate to examine the status of privacy in both the public and private sector and to recommend specific legislative or administrative action to enhance its protection. Indeed, the President's Domestic Council Committee on Privacy, established in early 1974, immediately perceived the need for a comprehensive survey and analysis of existing and planned data banks and of the laws pertaining to privacy, confidentiality and security. That Committee realized, however, that such a task would be time-consuming and difficult. It relied, therefore, on a recent survey of Federal data banks conducted by a congressional committee. The Privacy Committee of the Secretary of Health, Education, and Welfare had a similar experience. Similarly, a number of Department heads in recent years have discovered that they lacked concrete and comprehensive information about their own agency's systems. Since existing executive offices have neither the authority, nor the practical ability and resources to perform such functions, the Committee decided that it was necessary to create the Privacy Commission and charge it with these tasks. In doing so, the Committee has adopted a recommendation made by numerous experts and study panels for almost a decade.

The Commission is directed to complete the privacy study not later than three years from the date of its organization. It is authorized to make periodic reports of its findings to the President and to the

Congress, which will allow it to submit reports and specific recommendations on subject areas as they are completed, and not all at once at the end of its term.

The reports shall include recommendations for applying the requirements and principles of the act to the information practices of organizations under study, whether by legislation, administrative action or by voluntary adoption of those requirements and principles.

Need for Study

Governors and other State and local officials have cited the dearth of information about the practices of regional or national data banks which, because of their interstate nature, are difficult to analyze or control by State privacy laws and regulations. It is thus expected that the Commission's studies, especially those aspects analyzed by States, will assist the States in their own efforts to protect personal privacy.

Representatives of private industries, businesses and organizations have also indicated that such a study would better enable them to meet their ethical and legal obligations to protect individual privacy in an information-rich society while taking full advantage of the benefits of computer technology.

Guidelines for Study

The Committee is aware of the range of possible areas for investigation and of means of conducting such study. Therefore, subsection (b) establishes restraints, limitations and certain research guidelines for the Commission study so that the final product in each case may be responsive to the particular legislative and administrative needs of Congress, the executive branch and agencies of State and local governments.

As a specific requirement, the Committee is to examine and analyze the interstate transfer of information about individuals whether by manual or electronic means. As an example, interstate corporations and multi-state governmental units and private regional data banks exchange among themselves a wide variety of information about people for the purpose of approving credit applications, hiring personnal, examining claims for insurance, and other transactions affecting decisions about the rights, privileges or benefits of individuals. A second example would be the experimental Electronic Funds Transfer System now being developed under the auspices of the Department of the Treasury and the Social Security Administration to electronically transfer social security benefits and other welfare payments from government to bank.

The Commission study is by no means directed to all data banks on people or all personal information systems. Rather, the Commission is charged to study only those which significantly or substantially affect the privacy and other personal and property rights of citizens. The Committee has heard and reviewed much testimony which indicates that interstate and national information networks affect the lives and substantive rights of individuals in a variety of ways. The Committee believes that the Commission should focus its attention on the affects of the collection, use, storage and transfer of information on the rights of individuals.

Social Security Numbers

Particular practices and subjects which the Committee has found are of special concern to the public are designated to be given priority. The Commission is required to study the use of social security numbers, license plate numbers, universal identifiers, and other symbols used to identify individuals in information systems and to gain access to integrate or centralize systems and files. One of the most important problems that has arisen in the Committee's consideration of privacy legislation is the built-in potential among personal information systems for the creation of a national data bank. A single national system utilizing information gathered about individuals from many sources could be advanced by the use of a common identifying number or symbol unique to each individual. The Committee intends that the Commission examine the use of social security numbers and other similar identifying symbols or codes in light of their possible use as universal identifiers, or as indexing tools which may ease the breach of confidentiality or make government record surveillance over the individual easier. The Commission should review laws, regulations and decisions affecting these matters and, in particular, examine the costs and feasibility of halting or restraining present trends in such practices and developing less threatening alternatives in the interest of guaranteeing individual privacy and confidentiality of personal information.

Statistical Data

The Commission is also required to study the matching, integration and analysis of federally produced statistical data with other sources of personal information to reconstruct individual responses to statistical questionnaires for uses other than those for which the information was collected. The Committee was presented with circumstantial evidence in Volume II of the 1971 President's Commission on Federal Statistics which indicates that it is possible, through sophisticated computerized techniques to estimate with reasonable accuracy personal information relating to identifiable individuals using multiple sources of statistical and nonstatistical information published by Federal and State agencies. Such information yields to its user significant information about individuals heretofore held in confidence and thus violating a pledge of confidentiality made by Federal agencies collecting the information for statistical purposes. Commercial firms are rapidly improving this technology, thus creating the need for careful attention to its direction and ultimate capability and its impact on privacy. The Committee intends that particular attention be paid to such developments by certain direct mail marketers, and that the Commission recommend measures to preserve the guarantees of confidentiality provided by existing census statutes and regulations and promised by organizations conducting statistical surveys.

The Committee believes that legislation on privacy issues should give due regard to the preservation of the Federal system and should allow States to provide stronger controls as they see fit or to experiment with their own legislation to meet problems unique in those States. At the same time, they should be afforded all of the information which such a national study can make available. In conducting its study, the Commission is required to examine the laws, Executive

orders, regulations, directives, and judicial decisions which govern the activities under study by the Commission and determine the extent to which they are consistent with the rights of privacy and due process, and other guarantees of the Constitution which this Act seeks to promote. The Committee is cognizant that many laws, regulations and judicial decisions affect the collection of information about individuals and the rights of individual privacy. To fully exercise its study function, the Committee feels that the Privacy Commission should examine these and take them into account as necessary in making its recommendations. In acquiring such information, the Commission may seek the advice and aid of governors, attorneys general, judges, mayors and others with unique control over or knowledge of the public policy and law on privacy matters.

Federal-State Relations

The Commission is directed to determine the extent to which major governmental and private personal information systems affect Federal-State relations or the principle of separation of powers. The Committee believes that many of the personal information systems funded or otherwise sponsored by the Federal Government subtly affect the ways that State governments are able to operate their own information systems and interact with the Federal Government. For one example, a Federal information program that solicits certain types of information about individuals from State governments might also prompt those State governments to begin collecting the same type of information, for their own, perhaps undetermined, uses, without appropriate guarantees of confidentiality. On the other hand, a Federal program may, because of its unforeseen results, be effectively prohibiting the State from adequately promoting the privacy of its citizens, the confidentiality of data about them, or the security of its automated data systems. Where necessary, the Committee intends that the Commission examine the often unforeseen results of Federal-State information-sharing in light of their potential affects on Federal-State relations.

For each matter under study, the Commission is to consider public policy and current standards and criteria governing the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information. The Committee heard testimony and has reviewed much material indicating that many information users already impost strict safeguards and confidentiality requirements on their information systems. The Committee wishes the Commission to be able to review these rules and practices in order to determine the scope of their use and their effectiveness as models under particular legislative schemes.

The Commission is also specifically directed to include in its study certain areas which have been shown to be of concern to the public and to legal commentators on privacy issues. These include informational activities in the areas of medicine, education, insurance, employment and personnel, credit, banking and finance, travel, hotel and entertainment reservations, and electronic check processing.

In addition to these, the Commission is authorized to study such other information activities as it believes are necessary to carry out the congressional policy of this Act. This provision is included to

assure that the Commission may be free to examine new developments in means of sophisticated surveillance techniques or of transmitting personal information by satellite and other electronic means.

Exceptions to Committee Study

An exception is made to the Commission's study power for information systems maintained by religious organizations, in order to preserve the principle of separation of church and state. A similar exemption for charitable and political organizations was deleted from the original bill by Committee amendment to assure the broadest scope to the Commission's study for the protection of individual privacy.

This section requires the Commission, to the extent practicable, to collect and utilize findings, reports and research studies of congressional and State committees, other government agencies, private organizations and individuals which pertain to the problems under study by the Commission. The Committee recognizes that there has been much written and said about the issue of personal privacy, due process and confidentiality. In fulfilling its study mandate, the Commission must take full advantage of this research and information. In addition, there are available in computerized form the texts of statutes and judicial opinions.

The Committee expects by this requirement to have incorporated within the Commission study the most valuable aspects of previous research efforts and thereby reduce the administrative costs which a nationwide study might otherwise involve.

In many subject areas, the Commission may need to do no more to meet its obligations on some aspect of the study than develop and draft the specific language for legislative recommendations to be submitted to Congress and the President.

The Commission is also authorized to receive and review individual complaints with respect to any matter under study. This is to assure that wherever possible, the Commission's empirical research shall include, and the recommendations address, the complaints and concerns expressed by individuals or organizations. Frequently, the economic or political consequences of seeking redress from or complaining to the offending agency makes it difficult, if not impossible, for the individual to obtain remedies for invasions of privacy or for wrongs suffered by inaccuracies fed into computerized data systems. The Commission should not have to rely on reports of complaints made to the offending organization.

In addition, in some areas, the lack of sufficient technical and legal resources makes it difficult for Congress to investigate individual cases of information abuses which come to the attention of members to a degree sufficient to produce a record for complex legislation.

As indicated, the Committee does not intend such studies to be theoretical and speculative but to be based on legal research, review of data practices and particular data banks, and investigation of complaints it receives.

SECTION 107

REPORTS

Section 107 provides that the Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this Act.

48-610 O - 76 - 14

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

Section 201

Safeguard requirements for administrative, intelligence, statistical-reporting, and research purposes

Section 201 sets forth standards and procedures to govern all stages of decision-making for and operation of the information systems of each department and agency of the executive branch.

Subsection 201(a). This subsection is the provision of the bill specifically directed to the constitutional and legal control of the invasion of individual privacy by government. It reflects the intent of the Committee to follow the recommendations of the report of the National Academy of Sciences, that "in terms of privacy there should be a general policy to extend the zones of personal and group freedom from compulsory data collection so that matters that ought not to be considered in making decisions about individuals do not become part of the formal record at all."

Beyond that, this section, together with subsection 201(b)(1) and (7), reflects another dimension of the privacy issue, which is that, under our Constitution, there are, or may be, some human activities of which Government should not take note for any purpose at all because of the detrimental effect on freedom, and that this is true whether or not the information is intended to be used to make decisions about specific individuals.

This section reflects the Committee's effort to insert considerations of privacy in the decision-making process involving management of information systems. As the Academy report states, privacy is "the primary civil liberties issue, since both confidentiality and due process questions disappear if the data are not gathered in the first place, or once they are destroyed."

The section is designed to insure that a Federal agency weighs strongly the rights of personal privacy against its authority and need to gather personal information for a public purpose. Before an information-gathering program may be implemented, the agency must make a determination that its action is authorized and warranted to carry out a statutory obligation. This provision affirms a basic principle of good management in public administration in that it is designed to require that the kind of information about individuals which an agency seeks to gather or solicit, and the criteria for programs to investigate individuals will be, judged by an official at the highest policymaking level to be relevant and necessary to a statutory purpose of the agency.

The section is designed to implement the following policy judgments in the report:

> Not only should the need for and relevance of specific items of personal data have to be established in positive terms but serious consideration should be given to whether some entire record-keeping programs deserve to be continued at all; this was the basic question raised about the Army's domestic intelligence watch over civilian political activity in the late 1960's. A further consideration where need for collecting data

> is at issue is whether records should be retained beyond their period of likely use for the purposes for which they were originally collected.
>
> A related but more complicated question concerns the continued existence of files of information which is no longer supposed to be used for making decisions about individuals. Many cumulative records about individuals in various sectors of the organizational world are filled with facts and evaluations set down in an earlier time, under a different socio-political ethos. In this setting, it is not enough to say "from now on we will not . . ."; steps need to be taken to remove from historical records in high schools, colleges, commercial reporting agencies, law-enforcement files, and other organizations the personal information previously gathered about political, racial, cultural, and sexual matters that would not be put in the files under present rules. To the extent that evaluators today have such records to consult, especially for decisions that are not visible to the individual, the presence of such information represents a dead (and improper) hand from the past.

Most of these provisions contain terminology which will allow administrative definitions to fit particular agency needs and programs. They are intended to be implemented by the model guidelines developed by the Commission which may then be adopted by the agencies or altered as found necessary. This will, for instance, allow for development by Commission experts, in consultation with other Federal officials, of careful, workable definitions of such terms as "accurate," "timely," "complete," and "relevant."

Such a process is also envisioned for determining precise details of the contents of the notices of data banks required to be filed for the Federal Register and with the Commission. These can be discussed and determined with the assistance of the Commission in accordance with an agency's unique problems and record-keeping methods.

Subsection 201(a)(1). Provides that each Federal agency shall collect, solicit and maintain only such personal information as is relevant and necessary to accomplish a statutory purpose of the agency.

This section, therefore, governs the first phase of the process which is the gathering of the information in the first place. The provision reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statute. Second, it requires a decision that the collection of information or investigation of people along certain information lines is necessary in that the needs of the agency and goals of the program cannot reasonably be met through alternative means.

Where there are difficulties in linking a personal data program to statutory authority, it is to be expected that some agencies may face hard decisions of whether or not to seek additional authority, to reject certain programs entirely or to alter investigative standards.

A third element in this decision process is the fact that the information which officials propose to collect must be maintained and

integrated into the agency record-keeping system. Thus the decision on the relevance and need for certain gathering of information and investigating of citizens requires consideration of how that data will overlap or conflict with existing data banks and information programs of the agency.

This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary, but rather, must be authorized, and found to be not only reasonable, but warranted by the overriding needs of society as the agency is responsible for administering to those needs.

The provision is the legislative reflection of the conclusion of a panel of the Committee on Scientific and Technical Information of the Federal Science Council which recommended that "an agency should formulate as precisely as possible the policy objectives to be served by a data-gathering activity before it is undertaken. Agencies are encouraged to think carefully about the legitimacy of the activity, the significance of the data for the agency's program, the potential burden on the respondents and the possible availability of the data from some other source. This may make it possible to achieve a reduction in the burden being put on citizens and to harmonize governmental questionnaires and surveys. Great care should be exercised in framing information requests to be certain that the desired information is captured initially and that multiple requests for information is captured initially and that multiple requests for information are avoided, and that no more sensitive personal information is collected than necessary."

Subsection 201(a)(2). Provides that each Federal agency shall collect information to the greatest extent practicable directly from the subject where the information may result in adverse determinations about the individual's rights, benefits, and privileges under Federal programs.

This section, as originally introduced, had no qualifications, but reflected the basic principle of fairness recommended by several reports, that where government investigates a person, it should not depend on hearsay or "hide under the eaves", but inquire directly of the individual about matters personal to him or her.

In order to meet agency objections about the needs of certain civil and criminal law enforcement programs requiring intelligence and investigative information to be collected from other sources, the section was limited to instances where the information sought could affect a person's qualifications to be considered by government for employment or other rights, benefits and privileges. This is the minimum standard of fair procedure, although there may be instances where it cannot be observed. It is expected however that these will be kept to a minimum. Cases may arise for instance, where it is not practical (1) for logistical or financial reasons, or (2) for reason of conflicting, more restrictive, statutory requirements which cannot, after consultation with the Commission, be resolved, or (3) where the information is on hand from other disclosures made by the individual and he has specifically consented at the time of disclosure or later to have it used for other or related purposes within the agency or by another agency.

At the same time as it assures accuracy and fairness to data subjects by this provision, the Committee does not wish to defeat the purposes of the Federal Reports Act to promote the efficient, economical exchange and sharing of information; nor does it wish to impose undue burdens on individuals from whom information is solicited. However when the cause of ordinary efficiency and small economies is weighed against the interest of personal privacy and confidentiality of sensitive information, the Committee expects the balance would tilt in favor of the latter. However, the Act looks to a conscientious weighing of the interests by administrators, and to decisions made on the record pursuant to the discretion allowed by this section.

Even where information is acquired from other sources, an agency should, in the interest of the standards of accuracy and efficiency to be promoted under subsection 201(b) make efforts to have it reviewed by the subject individual. For example, by sending him a copy of the information and affording him an opportunity to affirm, deny or explain it. Such review may constitute compliance with subsection 201(a)(2). This section reflects the committee's adoption of the conclusion of the COSATI panel that "Information should not be collected on a hearsay basis or from people who have only a tenuous association with the data subject and therefore are not in a position to report data from a high probability that it will be accurate."

Subsection 201(a)(3). Requires that each Federal agency shall inform any individual requested to disclose personal information for any purpose whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, will result from the nondisclosure, and what rules of confidentiality will govern the information.

This requirement, in various forms, has been universally recommended by commentators and government and private groups, the HEW Report, information specialists, congressional witnesses and others, as basic to the protection of the individual from the arbitrary information power of the Federal Government.

The Committee intends it to remedy the many documented complaints from citizens that they were pressured, coerced, or induced by deceptive means into responding to governmental questionnaires seeking highly personal information for administrative programs, or for census and other statistical and research purposes of the Federal agencies; that they were not told and, furthermore, were frequently unable to learn, even with legal assistance, whether compliance was voluntary or mandatory, what statutes authorized it, what penalties attached to nonresponse, or exactly why the Federal Government wanted the information in the first place.

The section anticipates that Federal requests or requirements for personal information henceforth shall be accompanied by written or oral notices presented in obvious or highly visible manner, which use the specific terms "mandatory" or "voluntary" in describing the nature of the individual's desired response, and providing the other requisite information concerning the authority of the agency to conduct the survey, initiate the inquiry, or, in the case of administrative programs, to ask particular questions of the applicant. The Committee believes that an agency should be able to communicate to the individual, without intimidation, whether he is required to comply with

a request for information and what the likely consequences are of his refusal. To further clearify the consequences of these options, the notices should also include an explanation of the limits on the agency's ability to keep information confidential; for example, under compulsory legal process.

The Committee is not impressed with executive branch arguments and those of some information users which hold that such candor on the part of government represents "poor psychology" and will destroy the integrity of statistical surveys and other data programs, or that it will discourage cooperation with official inquiries. The Committee believes, rather, that just the opposite results will be obtained. Furthermore, the spirit of constitutional considerations of due process and self-incrimination should pervade the conduct of such inquiries for administrative, regulatory, or other such governmental data programs.

In defining the purposes of this section, the Committee endorses the recommendations of the HEW report that "the requirement is intended to discourage organizations from probing unnecessarily for details of people's lives under circumstances in which people may be reluctant to refuse to provide the requested data. It is also intended to discourage coercive collection of personal data that are to be used exclusively for statistical reporting and research."

We also endorse the explanation of the COSATI panel of the need for such protections to avoid "the use of coercion or intimidation in the course of gathering information." We agree with the Panel that: "unless disclosure has been made mandatory by Act of Congress, personal information must never be extracted from an individual without securing his informed, express consent * * * In gathering information from individual citizens, Federal agencies have an obligation to disclose to them the purpose for which the information is being collected, to state clearly the use or uses to which it will be put, to identify the governmental and non-governmental individuals and organizations that will be given access to it, and to indicate whether the individual's name will be associated, either directly or indirectly, with the information.

"The type of disclosure is particularly important when the individual's participation in a data-gathering activity is voluntary in character, and is one way of assuring that the voluntary consent of the individual is meaningful. It enables him to evaluate the risk he may be assuming by revealing personal information, and in some cases, permits him to weigh that risk against the advantages of participating in a particular governmental program. It also should contribute to preventing alienation and should encourage participation in the data-gathering process. For the same reasons, it is imperative that the agency's understanding with the individual be honored.

"When an individual is required to furnish information by act of Congress as is true for the decennial census, informed consent of the type described in the preceding paragraph is not necessary. Nonetheless, it is desirable to provide individual respondents with as much information concerning the data activity as possible."

Of particular concern to people subjected to governmental inquiries is the general lack of precise information afforded at the time of collection about the penalties for and consequences of nondisclosure. Where compliance is mandatory or where untrue response is punishable, with

penalties ranging from $100 to $500 to $1,000 and a year in jail, basic due process principles require that the individual be put on notice of such penalties. The same constitutional considerations require that where such penalties accompany demands for personal data, that demand must be based on statutory authorization.

The Committee considers it basic fairness that any agency provide whatever information it has at hand about the immediate consequence of not responding to an inquiry or particular question. While it may usually be convenient to provide this warning on the face of a written inquiry upon initial collection, in some cases, the Committee recognizes that it may be more practical to supply such information promptly at a later time upon request of a data subject who may voice objection or concern about some phase of a written or oral inquiry, or to some particular question. Clearly, the agency cannot be reasonably expected to tell all foreseeable or imaginable consequences of nondisclosure or disclosure. It can however, advise when nondisclosure will preclude any consideration of an applicant for employment, or for a right, benefit or privilege, or when nonresponse may be accorded some weight in official consideration of the application.

To cite one example:

A Federal employee requested to complete a research questionnaire stating which political candidate he or she prefers should be told at the outset that the response is voluntary, that it will not affect employment, and will not go into any government file. However, even such notice will not preclude an employee electing to challenge the inquiry for possible violation of the limitation in subsection 201(b)(7) on inquiries on first amendment activities.

Similarly, couples applying for Federal housing loans have the right to know if they have to answer questions on whether they intend to have children and if they practice birth control, why the agency requires such information and whether or not they lose the chance for the loan if they don't disclose such information.

Subsection 201(b)(1). Requires each Federal agency that maintains an information system or file to insure, that is issue any requisite regulations, and take affirmative administrative action for the purpose of assuring, that personal information maintained in the system or file, or disseminated from it, is to the maximum extent possible, accurate, complete, timely and relevant to the needs of the agency.

This requirement complements that of subsection 201(a)(1) imposing such a duty on agencies and is deemed necessary to the effective exercise of any right of the individual to challenge a record, or a data bank on these grounds through the agency or the courts.

The standard of relevancy is that statutory basis for an information program required by subsection 201(a)(1). The scope of these two sections encompasses all phases of the information system. The standards of relevancy here relate to the constitutionality and legality of the entire information program, as well as, the reasonableness of maintenance or any particular piece of personal information, given the statutory jurisdiction of the agency. The standards of accuracy, completeness, and timeliness, as well as relevancy are directed to the quality of the information in an individual's own file. The section thus looks to a double-pronged consideration, first to the authorized needs of the agency, and second, to the scope of the administrative need for information in order to make a decision on that individual.

The condition that such a goal be pursued to the "maximum extent possible" is attached to promote an extra measure of caution and zeal beyond the ordinary standard of care which governs all other information handling. But it is also designed to allow the agency the freedom to determine through its own regulations and directives, as adapted from the Commission model guidelines, what is reasonably "possible" within the limits of the statutory duties placed on the agency, of its resources, of technological feasibility, and of administrative practicality. The Committee recognized, for instance, that it is administratively and logistically impossible to keep current and timely the statistical information maintained for historical and archival purposes. Yet an agency may well question an investigative data bank or file on people which was long ago outdated and is now seldom used, and which services no program or one which is maintained only in case the individuals once again deal with the agency. It is hoped that with the inclusion of such a broadly-termed mandate linked to the right of the individual to challenge, there will begin a long-overdue evaluation of agency program needs for stale, irrelevant, and untimely information.

When combined with the subsection 201(a)(1) duty to confine information gathering to only personal information relevant and necessary to accomplish a statutory purpose, the Committee has provided agencies and the courts with a standard against which the individual may challenge information in a file or data bank.

Subsection 201(b)(2). States that agencies shall require employees to refrain from disclosing records or personal data in them, within the agency other than to officers or employees who have a need for such record or data in the performance of their duties for the agency

This section is designed to prevent the office gossip, interoffice and interbureau leaks of information about persons of interest in the agency or community, or such actions as the publicizing of information of a sensational or salacious nature or of that detrimental to character or reputation.

This would cover such activities as reading results of psychological tests, reporting personal disclosures contained in personnel and medical records, including questionnaires containing personal financial data filed under the ethical conduct programs of the agency.

It is designed to halt the internal blacklisting that frequently goes on in agencies and on Federal installations on persons who do not comply with the organizational norms and standards for some reason, such as not participating in savings bonds drives or charity campaigns; and the listing of results of employee tests or performances;

It is designed to help prevent the easy exchange of data about the same individual between regional managers of different programs within a bureau or department and the consequent informal or inadvertent administrative integration of data for purposes of making a governmental decision about that person. This might be true, for instance, of a farmer who had filed information or been the subject of official inquiry in several agricultural programs in one county.

The section envisions that if an employee dealing with official information about a person is requested to surrender that person's record to someone who clearly has no need for it, he should decline or seek to define the purpose of the requested disclosure. One of the

results of this section may be to promote a sense of ethical obligation on the part of Federal officials and employees to ascertain when improper disclosure of information within the agency may be sought or promoted for personal, political or commercial motives unrelated to the agency's administrative mission.

It is not intended to conflict with other statutes, rules and regulations governing employee conduct or information practices but is meant to implement and reinforce them. The standard of refraining from certain behavior implies, by definition, not indulging in impulses to engage in positive behavior to the contrary, in this case, in not taking positive action or making specific administrative or personal efforts to disclose personal information acquired in the course of one's duties when such disclosure is not required.

Subsection 201(b)(3). Requires any Federal agency that maintains a personal information system or file to maintain a list of all categories of persons, including individuals and agencies authorized to have regular access to personal information in the system or file.

The original bill required Federal agencies to record each and every access to any information system or file. By requiring instead simply a list of the categories of employees and of other agencies and persons who on a regular basis are permitted to examine files within a system of personal information, the bill meets the objections of agencies that a strict accounting of every access was not administratively practicable or feasible in view of the necessary routine in daily access to a file by varous identifiable groups of people and by many employees for purposes of entering or withdrawing information. The problem of requiring identity and purpose of access by reporters and others in the public exercising inspection rights under that and other acts made it more feasible to require a list which would be available to the public and to individuals who are subjects of the files.

Where employees are concerned, the kind of list envisioned would make it possible to identify for any particular day the employees occupying a position and performing duties requiring such access to a particular file or authorized to have such access. Since this is deemed merely good management and responsible personnel practice for all Federal systems and is a practice observed in many agencies anyway, it is not expected to present difficulties in compliance.

With regard to the definition of who are "regular" users beyond the agency, outside of the public and press, the type of regular use envisioned is that such as where, by statute and written agreement for information-sharing among agencies, there is access by terminal for the purpose of implementing such agreement. The Commission, in the course of developing model regulations for guidance of agencies in implementing the Act, will assist in promoting a workable definition of such users by reference to the specific situations presently authorized.

Subsection 201(b)(4). Requires any Federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access granted to the system, and each disclosure of personal information made to any person outside the agency, or to another agency, including the name and address of the person or other agency to whom disclosure was made or access was granted. An exception is recognized for those accesses and disclosures involved in public inspection or copying

pursuant to law or regulation, which includes the Federal and State open records laws and regulations implementing them.

This section is included as an essential element of the Code of Fair Information Practice and the "Information Bill of Rights" in order to promote the full implementation of the right to seek to obtain a meaningful correction of inaccurate records, not only in the offering agency, but wherever in government and private organizations the inaccurate information may have been transmitted.

The kind of audit and "audit trail" envisioned here is one that makes it technically and administratively possible to audit and inspect the nature and pattern of transfer of personal information whether in manual or computerized form outside the agency system, to be integrated in another agency's system, or to other persons in other agencies of government.

Furthermore, such record of access and disclosure helps assure against administrative departure from the stated uses, access controls, and users required to be filed in the Federal Register and with the Privacy Commission, and to guard against illegal seizures of information. It is designed to make oversight of information practices of government more manageable and efficient.

Subsection 201(b)(5). Requires a Federal agency that maintains a personal information system or file to establish rules of conduct and notify and instruct each person involved in the design, development, operation, or maintenance of the system or file, or in the collection, use, maintenance, or dissemination of information about an individual, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance. This notice would include consultants, contractors, and those outside the agency involved in such activities.

This section, another essential element in the Code of Fair Information Practice, merely recognizes principles of good public administration that the most effective hierarchial management of an organization results from informing employees of their responsibilities and how they relate to overall agency obligation and of their duties regarding the information they process and to the techniques, equipment and instruments with which they carry out their assignments.

While most agencies may have ethical conduct rules with respect to the information under the control of civil servants, these do not necessarily always reflect the ever-expanding information needs of government or the increasing mechanization and computerization of government records, with the vast numbers of specialists and technicians brought rapidly into Federal agencies to deal with them. Nor do these codes reflect the developing professional codes of ethical conduct for those involved in application of computer technology and sophisticated information-processing techniques in the public and private sectors. It is expected that the Commission, in drafting its model guidelines, would incorporate these and would encourage their more extensive adoption by agencies in their rules implementing the Act.

This section thus envisions positive action by the agency, beyond mere publication of implementing regulations, to notify people administratively, perhaps by a handbook for which each person is responsible, and by a special session instructing them on changes made in existing programs by the new Act. It is expected they would be in-

formed of administrative sanctions and other penalties applicable by reason of statutes and regulations governing performance and behavior of Federal personnel.

Subsection 201 (b)(6). Requires any Federal agency that maintains an information system or file to establish appropriate administrative and physical safeguards to insure the security of the information system and confidentiality of personal information processed and handled in it and to protect against any reasonably foreseeable or anticipated threats or hazards to their security or integrity which could result in substantial harm, embarassment, inconvenience, or unfairness to any individual on whom personal information is maintained. [The analysis of this subsection is supplemented by that for subsection 201(f).]

Once privacy, confidentiality and due process policy issues have been resolved, the administrative measures and technical features needed to implement those decisions are required to be taken by the agency under this section. These may include, for example, establishing and enforcing rules of access, adding computer software that appropriately screens requests for access and that keeps accurate and complete records of access and disclosure, and installing locks and similar security devices. Many agencies will no doubt find their present measures adequate for many existing systems and files. Others may need supplementary action. All must make such considerations part of their decisions to create new systems and data banks.

The Committee recognizes the variety of technical security needs of the many different agency systems and files containing personal information as well as the cost and range of possible technological methods of meeting those needs. The Committee, therefore, has not required in this subsection or in this Act a general set of specific technical standards for security of systems. Rather, the agency is merely required to establish those administrative and technical safeguards which it determines appropriate and finds technologically feasible for the adequate protection of the confidentiality of the particular information it keeps against purloining, unauthorized access, and political pressures to yield the information improperly to persons with no formal need for it. Once it determines the need for certain physical and technical features for the computerized or mechanized stages of their systems, or for their manual files, agencies would be expected, in compliance with the Act, to seek such features where necessary through the budget process or as alternatives to existing methods.

The Committee is cognizant of the advice of the Director of the National Bureau of Standards Institute for Computer Sciences and Technology, and intends that the term "appropriate safeguards" should incorporate a standard of reasonableness and "refer to those safeguards which represent current state-of-the-art procedures at any given time, despite any weaknesses that may exist in the technology at that time." However, the Committee does not intend to discourage the active pursuit of new and more useful safeguards.

While this interpretation represents a retreat from the absolute requirement of obtaining such technological features, the Committee agrees that given present cost factors and considerations of economy, such an approach suggests that we could look forward to increasingly higher standards of 'reasonableness' as new technologies are further developed to make our systems progressively more secure. But it

would also permit the immediate application of all of these techniques where they can contribute—even in their present form—to better protection of data confidentiality and individual privacy.

The Act thus provides reasonable leeway for agency allotment of resources to implement this subsection. At the agency level, it allows for a certain amount of "risk management" whereby administrators weigh the importance and likelihood of the threats against the availability of security measures and the consideration of cost.

The Act makes the wisdom and legality of these decisions reviewable by the Commission and Congress where they involve major changes in computerization and file management of data on people. It thus makes Congress, with the advice of the Commission, the final arbiter of the decision weighing cost, economy, technological feasibility against privacy and other civil liberties.

The Committee is furthermore aware of the problems of requiring computers dedicated to one use or one sensitive category of information. Further, it agrees with the National Academy of Sciences Report that "it would hardly advance civil liberties in this country, if in the name of protecting confidential files, civilian government agencies and private organizations were to adopt the authoritarian environments and intrusive personnel policies used by defense and intelligence agencies to safeguard their information systems."

The Committee was persuaded on the need for such standards by the testimony of computer experts and by reported cases of file by theft, tapped transmissions and disclosure problems in the use of time-sharing facilities. As the National Academy report recommendation summarizes numerous expert opinions:

> Both managers and policymakers should be aware that the payoff in sensitive personal information to be obtained by insiders violating confidentiality rules and outsiders breaching system security is going to increase in the coming years. More comprehensive information about people will be collected in the kind of large-scale record systems that are growing up, such as the omnibus charge-card systems and national welfare assistance programs. Furthermore, as more organizations make use of the low cost and flexible services that are available in commercial time-sharing facilities, more high-payoff targets such as the membership and contributor lists of various kinds of organizations will be appearing in time-sharing systems, requiring more attention to the security problems in multiple-user commercial facilities than this area has received thus far. (Report, p. 395)

The range of alternatives available to agencies to promote adequate systems security has been described at length for the Committee record and in other congressional hearings. For convenience and expertise, the National Academy of Science report can be cited here as indicative of the Committee judgment that it is not tying the administrative or logistical hands of the executive branch with strict impossible standards, but is leaving it for the agencies and the Federal Government to request needed specific features from manufacturers in the course of the Federal procurement process. The report states:

> What seems clear is that adequate computer technology already exists to provide both the hardware and software protections that are needed to afford effective levels of security for personal data in the kinds of record systems we have been considering. To give several examples of particular relevance to civil liberties issues, much more could be done by computer manufacturers to put record-field access control features into the software operating systems of computer systems, so that users could exercise greater control over the authorization tables that govern access to the data base for each user. Similarly, much more could be done by software developers to provide the programs for real-time monitoring against unusual volumes of use or unusually low yields of 'hits,' in order to warn systems managers about what may be unauthorized uses or improper 'browsing' in sensitive files. (Report, p. 395)

The Committee does not, therefore, mean to relieve any administration officials of responsibility for promoting the purpose of this subsection. We are aware of the availability of administrative and technological means of promoting this purpose, and are mindful, in particular, of Justice Department technical reports by the Project SEARCH Group and reforms effected by law in the computerized information systems of the States of New York, Massachusetts, Minnesota, and others.

The Committee has taken note of laudable activities in the executive branch to foster administrative observance of standards of confidentiality of information and systems security. Such efforts and management guidelines have heretofore been dependent upon the good will of officials of the department and agencies and upon their zeal, time and discretion in use of resources. This Act will not impede these efforts, but will provide the needed legal support to aid in their achievement.

Subsection 201(b)(7). Provides that no Federal agency that maintains a personal information system or file shall establish any program for the purpose of collecting or maintaining information describing how individuals exercise rights guaranteed by the first amendment unless the head of the agency specifically determines that such program is required for the administration of a statute which the agency is charged with administering or implementing.

This section combined with the application of the principles of relevancy under subsection 201(a), reflects the preferred status which the Committee intends managers of information technology to accord to information touching areas protected by the First Amendment of the Constitution. It is aimed at protecting Americans in the enjoyment of the privacy of their thoughts, habits, attitudes and beliefs in matters having nothing to do with the requirements of their dealings with an agency seeking information. It is designed to assure that where such investigations are undertaken, the decision is made by a responsible official who is accountable on the record rather than by the culminative ad hoc, case-by-case decisions of investigators and drafters of questionnaires which can easily become the common law of an agency's practice in lieu of agency-level decisions.

This section is directed to the planning stage of any executive branch programs being designed for the principal purpose of identifying Americans who exercise their rights under the First Amendment and of taking note of how and when such activities are exercised. It is directed at programs which would (1) require gathering of such data from other agencies or (2) would require questions to be asked of the subject individual or of others about his or her personal political beliefs and philosophy, about legitimate activities of the individual in participating in community events, in religious practices, in seeking redress of grievances through such methods as signing petitions to be sent to Government agencies, Members of Congress or State legislatures; picketing under lawful circumstances; associating with others of like mind for the purposes of exchanging social, economic or political views; engaging in lawful demonstrations with others of like mind for the purpose of expressing opinions about governmental, social or economic policies; or expressing written or spoken opinions about such matters through the press, including letters to editors and comments on radio and television programs.

This section's restraint is aimed particularly at preventing collection of protected information not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future. This, of course, applies not only to the agency's own programs, but also to its participation in such programs undertaken by other agencies.

It is directed to overly-broad inquiries made in the course of administering programs requiring judgments on individuals for determining employment and other rights, qualifications, benefits, or privileges under Federal statutes.

Next, the section is directed to inquiries made for research or statistical purposes which, even though they may be accompanied by sincere pledges of confidentiality are, by the very fact that government make the inquiry, infringing on zones of personal privacy which should be exempted from unwarranted Federal inquiry.

The initiatives for such programs can be highly visible within an agency. They have come to the attention of Congress in formal regulations, in draft regulations, in informal directives and orders establishing programs or specifying certain criteria for gathering information deemed helpful to an agency. The requirements of this section, then, impose a duty on administrators to review such sensitive information programs at the earliest possible stage for their possible reception by the public and the subject individuals as threats to first amendment principles.

Since agency heads and administrators who may doubt their authority will consult their general counsels and the Attorney General as chief legal officer of the Government, it is expected that this section will impose no onerous burden on decision-makers. It is further expected, however, that not only the rigid letter, but the spirit of the Bill of Rights will prevail in their decisions and that where there is dispute about whether to solicit or try to collect the information, the scale will tilt toward observing the privacy of citizens and toward seeking alternative methods of fulfilling the administrative goals of the Federal Government.

The Committee does not expect that compliance will be met by a one-time administrative finding that an agency requires such information. Instead, there are expected to be specific determinations for new programs or alterations in existing ones, for directives on investigative standards, and for specific inquiries to be included on questionnaires sent for administrative, statistical, or research purposes.

The standards are applicable whether the information is sought for another agency's list, or by means of investigative questionnaire, lie-detector, oath, personality test, or any other similar technique.

Such determination will of necessity require reference to requirements of authorizing program statutes, "housekeeping statutes" of the departments and agencies, and pertinent judicial decisions. At a minimum, it expects that compliance will begin with creation of a special reviewing process for such matters at the highest level in each agency and that efforts would be made to seek to learn reaction to similar programs by Congress, the press and public.

Where authority is found to be lacking to make such inquiries as are deemed necessary for a statutory purpose, nothing prevents a department or agency from proposing to the President and from seeking of Congress legislation granting the requisite authority.

In drawing the particular restrictions on data gathering set forth in this section, the Committee does not intend to preclude future decisions that other types of personal information shall not be collected by Federal agencies.

Notices

Subsection 201(c). Provides for the notices describing the personal information systems and data banks maintained by the departments and agencies of the executive branch.

The provision incorporates the recommended language contained in the draft administration bill, and specific recommendations of the HEW privacy committee. The duties herein are required to enable the privacy commission to carry out its duties, as discussed above, pursuant to subsection 103(a), of publishing the Federal directory of personal information systems and data banks.

It is the Committee's intent to specify separately each matter to be included or considered for inclusion in such notices. The categories, however, are broadly stated to allow agencies to adapt their statements to fit their particular systems and files.

The Committee intends that no agency should be exempt from the requirement to develop such information needed for the required notices and to send it to the Commission. In addition, agencies are required to provide such information for publication in the Federal Register simultaneously when the Act becomes effective. Annually thereafter, they are to supplement such notice or, if there has been no change in their personal information systems or data banks, they should either state this or reissue their previous statement. While such simultaneous action may cause an initial logistics problem, the Committee believes it is necessary if the public notice function and the exercise of the rights which it serves are to be meaningful. Congress has received complaints about the difficulty which organizations and individuals have in keeping track of the scattered, obscurely-worded public notices filed by agencies which may affect privacy and civil liberties. In addition, citizens have complained that regional and

local employees of the agencies do not have available in their offices sufficient information about other data banks, investigative or data-collection programs, or information practices of their departments or agencies.

Since the Federal Register is not always available to the average citizen and since the urgency of a problem might preclude his seeking information from the Commission's guide to data banks, the Committee intends that notices with the requisite information should be available for distribution upon request.

It is expected that the contents of notices filed with the commission would of necessity be more detailed and elaborate than that provided for such agency distribution. Such a document might be abbreviated with an indication of where the individual may seek additional information.

The notice to the Commission should contain a listing of all statutes which require the collection of such personal information by the agency. This is to enable the Commission to carry out its function pursuant to subsection 103(a) to publish such list for each data bank and personal information system. This requirement was included by Committee amendment so that Congress and the public may know whether or not the agencies are collecting the information at the discretion or whim of administrators or if there is some statutory basis for it. This requirement to provide such legal data on a systematic basis will enable Congress, if it so desires, to reexamine or modify such statutory authority. Such information on hand will also assist the Commission in its investigation of the complaints of violations of the Act, and in its study of the practices of State and local and private sector organization in which it is to review the statutes and legal authorities for data programs.

Subsection 201(d). States the basic right of the individual to inspect and correct the personal information which the Government has on record about that person. Its provisions are minimum standards and are not intended to preempt or preclude laws and regulations providing even stronger protections for such rights.

These provisions reflect the cumulative recommendations of many experts in constitutional law and of governmental and private groups studying the issues of privacy and due process over many years. They also take into account experience with access and challenge provisions of the Fair Credit Reporting Act, as well as the many recommendations from the Federal Trade Commission, the public, and Members of Congress for strengthening and clarifying that Act.

As originally introduced, the bill provided that each agency notify all individuals about whom personal information is kept in the organization's files. This provision would most clearly have guaranteed that each individual would know what files of personal information are being kept, and by whom, and for what purposes. However, the Committee recognizes the merit of the objection raised by Federal agencies that individual notification would be unjustifiably costly. The Committee relies instead on the initiative of concerned individuals to learn whether they are the subject of government files. Using the Directory of Information Systems as a guide, any individual that writes a letter to any department or agency or official of the Federal Government asking to know what files exist on him shall receive a full

accounting, on behalf of the addressed department or agency and all of its subsidiary governmental organizations, grantees and contractors, of precisely what files do exist.

Subsection 201(d)(1). Requires each Federal agency which maintains an information system or file to assure that an individual who requests them may exercise rights set forth under this subsection. This requirement of "assurance" means no more nor less than that an agency must (1) issue appropriate implementing regulations and (2) take affirmative actions to apply them.

First, the person has the right to be informed of the existence of personal information on him or her, to know whether or not the agency even has a separate file.

In addition, full access to that file is to be afforded and the right to inspect it in a form which is comprehensible. This means that, unlike the existing practice in some agencies and under the Fair Credit Reporting Act, a person does not have to rely on a clerk's review of the file and a summary of what is in it. In addition, an agency may not just present a punched card or a collection of symbols on a print-out from a computerized system, or shorthand notes, but rather, must see that the information is presented in a form which the layman may reasonably understand.

The Committee agrees with the definition of "inspection" provided by numerous reports on privacy and summarized by the Academy of Sciences Report in the following terms:

> . . . where government files are concerned, we think inspection should mean the right of the individual to see a copy or display of the actual record in full, and to obtain an official copy of it for a nominal fee. Having an official describe the contents of the record to the individual but not let him examine it himself does not meet the test of openness or provide the psychological sense of having satisfied oneself about what is really there. (Report, p. 370)

The person is entitled to know the names of all recipients of personal information about such individual, including the recipient organizations and their formal or informal relationship to the system or file, and the purpose and date when the information was given out. This requirement would not apply, of course, where the accounting of access and disclosure under subsection 201(b)(4) need not be maintained because of the exemptions provided in subsection 202(b). It would involve allowing the individual to examine whatever access log is maintained for the file, together with a list of organizations exempted from entry in any log.

The individual also has the right to know the sources of the personal information. If such source is required to be kept confidential by statute, then the individual may be informed only of the nature of the sources.

The data subject may be accompanied by someone of his choice, in order to have the support or advice of a friend, relative, or attorney, in inspecting and evaluating the information and making his way through what may amount to a paper maze. The Committee believes this is necessary for effective exercise of rights under the Act. In some cases, the data may be so derogatory or otherwise sensitive from a privacy standpoint that the individual may be asked to furnish

63-610 O - 76 - 15

written permission authorizing discussion of the file in that person's presence.

The person has the right to obtain the disclosures and access required to be given under the Act in person with proper identification, or by mail upon written request. An agency may set reasonable standard charges for document duplication.

This section provides the further right to be completely informed about the uses and disclosure the agency has made of the information so that the individual may trace and correct the further uses of any inaccurate information, or take any necessary action to retrieve it from improper disclosure. The degree of "completeness," of course, would depend on what information the operative official has to his knowledge, or can reasonably obtain. In addition, the handling of such cases would be governed by the agency regulations defining what is deemed complete, timely and relevant to the agency needs in using the information for any purpose.

Subsection 201(d)(2). Describes the actions required of an agency as a minimum response to a person who lets the agency know in some oral or written fashion that he or she wishes to challenge, correct or explain personal information about that person contained in a system or file. Some statutory requirements or regulations may provide greater rights. These procedural rights are recognized as minimum in the recommendations of major commentators and studies. All of them are directed to implementing the basic principles of privacy and due process; that a Government agency should not take note of personal matters at all, and that it should, on the other hand, have information which is accurate and relevant as needed to make fair administrative decisions.

Subsection 201(d)(2)(A). The agency is to investigate the alleged inaccuracy by any reasonable means available and to record the current status of the personal information. Such investigation may require no more than a telephone call to another agency to ask them to verify the data. It may require no more than a review and recording of documentation, affidavits, authoritative materials, or records supplied by the individual. It may mean no more than checking other records and questioning investigators of the agency to clarify vague reports or correct inaccuracies. It may mean no more than reviewing the actions of a computer programmer who deleted or reduced to a minor role relevant information necessary to present a complete and fair account of a situation.

The agency regulations, with the guidance of the Commission's guidelines will provide standards for this and other actions of the reviewing official. The subsection is not intended to require an agency to extend its investigative powers beyond its statutory jurisdiction or beyond the reach of its fiscal and administrative resources. Rather, one of the purposes is to provide fairness to the agency by assuring that administrative means are afforded which allow the agency to protect itself from charges of inaccuracy and untimeliness by taking the necessary action to verify and update the challenged information.

Subsection 201(d)(2)(B). Requires the agency to correct or eliminate any challenged information that its investigation shows to be incomplete, inaccurate, not relevant to its statutory needs, not timely or necessary to be retained, or which can no longer be verified.

The finding of a need for retention can include the uses required by the agency's needs for meeting administrative, research or statistical obligations. The deciding officer should be able to do more than cite a presumed need; rather, the officer should be able to cite a statutory or other legal requirement supporting the decision.

Subsection 201(d)(2)(C). If the investigation does not resolve the dispute, the agency, under this subsection is to accept and include in the record of such information, a statement of reasonable length provided by the data subject setting forth his or her position on the dispute.

Wherever possible, such supplemental information is to be included or entered in the original file. In some cases, where computer programming already undertaken prevents the entry of such disputed information, it may be necessary to store it in a separate file, with an appropriate entry in the formal record of the existence elsewhere of relevant information.

Subsection 201(d)(2)(D). Requires the agency to report the challenged information and to supply the supplemental statement in any subsequent dissemination or use of the disputed information.

Following correction or elimination of challenged data, the agency shall, at the request of the individual, inform previous recipients of its elimination or correction. This requirement is not considered an unreasonable one since the data is conditioned and limited by the informed request of the individual who will have some knowledge of previous recipients and present users from exercising his right to know such matters under subsection (d)(1), and from inspecting whatever monitoring the agency is required to maintain under subsection 201(b) (3) and (4). In addition, the responsible agency officials will have discussed with the person the uses to which the data has been put, to their knowledge, and given him reliable advice on the need for pursuing the corrections with another agency or person. The provision is intended further to reduce the time and resources the individual must expend in correcting his records with each user, office, bureau or agency which may have received it. It will prevent the repetition of the access and challenge efforts for the same purpose.

No time limit was set on the provision, since it may be important to learn if one user received the data under some joint program ten years previous, while those disclosures made in the two years previous may be of no consequence. The deciding official should make some effort within an agency to trace formal or informal programs for exchanging or sharing data which would reasonably involve disclosures from the individual's file for any purpose.

Where such information would not be required to be kept before this Act or would not be kept under the exemptions of this Act, it would recognizably be impossible or difficult to comply with such requirements. In such cases, what is envisioned is a good faith effort to assist the individual.

Subsection 201(d)(2)(F). Establishes machinery for appealing and reviewing the failure to resolve a dispute or the decision of an official to deny a request to correct or supplement information.

Many scholarly proposals to afford the right of access and challenge of records have incorporated such a right within an administrative scheme giving the individual the right to appeal to an independent regulatory body. This was the intent of the original bill which gave

the individual the right to file a statement and provided appeal rights to the Federal Privacy Board, which had cease and desist powers.

The Committee, after considering testimony on the wisdom of alternative methods of regulation, decided against making the new Commission a Federal "ombudsman" complaint body, although it may now receive complaints illustrating patterns of violations of the Act.

Instead, the individual may seek review within the agency and direct judicial review by the Federal District Court in the event the agency rejects the challenge to its records.

At the request of the individual, the agency must provide a hearing within 30 days of the request and the individual may appear with counsel, present evidence and examine and cross-examine witnesses.

If, after such a hearing, the challenged record is found inadequate under 201(d)(2) then the agency must purge it from the file and from the agency system, or modify it as found appropriate.

The actions or inactions of any agency on a request to review and challenge personal data in its possession is made reviewable by the appropriate United States District Court by subsection 201(d)(2)(F)(iii).

The language of this subsection reflects that in an administration-sponsored omnibus criminal justice bill and was recommended by several witnesses and legal experts.

It is the Committee intent to substitute for regulatory agency review, a responsive speedy, agency process for resolving citizen's complaints about improper, illegal, or careless information practices of the Federal Government. Where many agencies may provide a review process after a harmful decision is made with the information, this section anticipates special initiative by agencies to extend existing processes, or to establish new procedures to encompass requests for access and challenge at an earlier stage in the management of the information.

As discussed previously, the Committee deems such access and challenge rights essential to enforcement of the Act, and as an aid to monitoring the system, and to promoting the reduction in the bulk of outdated, irrelevant files which agencies keep.

While agencies may exempt themselves through a rulemaking process, in certain areas, and with respect to particular records, the Committee does not consider the grant of such discretion a mandate to exercise it to the limit, but rather, to exercise it sparingly, with due regard for the principle of democratic government and the recognized right of all citizens to knowledge about the activities of government, a right more precious when the activities relate to information uniquely pertaining to the citizen.

Subsection 201(c). Provides for the coverage of the Act to apply to certain information systems or files of contractors and grantees or others when a Federal agency provides by a contract, grant or agreement for the specific creation or substantial alteration of such information system when the primary purpose of the grant, contract or agreement is the creation or substantial alteration of such an information system.

When such conditions apply, the agency shall, consistent with its authority, cause the requirements of subsections 201 (a), (b), (c), or (d) to be applied to such system and then only to the relevant portions

of such systems or data banks as are specifically created or substantially altered by such grant, contract or agreement.

In cases when contractors and grantees or parties to an agreement are public agencies of State and local governments, the requirements of subsections (a), (b), (c) and (d) shall be deemed to have been met if the Federal agency determines that the State or political subdivisions of the States have adopted legislation or regulations which impose similar or stronger requirements for the security of information systems and the confidentiality of personal information contained therein, and for the individual's right to have access to records and to challenge their accuracy.

Subsection 201(f)(1). This subsection is intended to assure knowledge by Congress, the executive branch, and interested groups of new Federal data banks and pooling of informational and computer resources to constitute centralized data systems not foreseen by Congress. It is to prevent a de facto national data banks on individuals free of the restraints on Federal power established by Constitution and statutes.

It is intended further to prevent creation of data banks and new personal information systems without statutory authorization from Congress and without proper regard for privacy of the individual, confidentiality of data, and security of the system.

The section therefore requires any Federal agency to report to the Commission, the General Services Administration, and to Congress on proposed personal data banks and information systems or files, on proposed significant expansion of existing ones, on integration of major files, on programs for significant records linkage within or among agencies, or for centralization of resources and facilities for automated data processing.

Explanation of this subsection should be supplemented by reference to the analysis of subsections 103(c) and 201(b)(6).

Such notices shall also describe the agency's judgment, positive or negative, of any effect it perceives that such proposal might have on the rights, benefits, and privileges under Government programs of the people who are the subjects of information involved in the change. For instance, does it mean that another agency which makes decisions on other rights of a person will now have terminal access to data of an agency for purposes of making its decisions and thus raise due process issues of relevancy? Will it allow creation of a data bank for investigative or intelligence, or research purposes which might, by its very existence, have an intimidating effect and raise first amendment questions of records surveillance? Will common storage facilities by agencies enable common usage not envisioned by the data subject or facilitate theft or improper access? On the other hand will the changes promote more effective exercise of individual rights, and fairness in decisions about the person?

What is anticipated is a check-off by the agency on the possible enhancement of or threat to the civil liberties and civil rights of citizens, including due process rights, from such changes.

The notice shall also state what administrative and technological features and measures are deemed necessary to protect the security of the information system or data bank and the confidentiality of the information. Such a statement should represent the ideal situation given the kinds of personal information and the promise of confi-

dentiality accorded it by law or by understanding with the subject individual. The report would then include the agency's best judgment on how best to achieve these goals within the limits of available technology, resources, and legislative authority. The subsection requires a description of the formal and informal actions, negotiations, and representations and their outcome, undertaken to obtain necessary features. This should include accounting of any consultation with computer and system experts, including the agency's own staff members and those employed by the National Bureau of Standards, the General Services Administration, by computer manufacturers, and professional organizations on computer and information technology; and any others within and without the executive branch, such as specialists in public administration and constitutional law.

The Committee recognizes that no level of security can be specified as absolutely adequate and that this often depends on what is available to promote the type of security needed for certain types of information.

It is expected that a set of criteria on the degree of sensitivity of personal data in the system would be developed on the basis of the historical breaches of confidentiality of that type of information. It is clear from the various public records and studies that there are some information systems in which there have been breaches for personal gain or political motives or other unauthorized purposes. There is clearly a need to safeguard these files as a first priority. The report to be filed with the Commission would detail the agency plan, given the historical threats or the likelihood of them. Clearly, the files in the Social Security Administration, while sensitive, might not have the same level of possible security breaches as the Passport Office Lookout File or the Civil Service Commission Investigative Index. Attached to that report would be the description of the agency's consultations with the National Bureau of Standards including any recommendations made by Bureau officials and other computer experts on desirable standards for safeguarding information.

Some unnecessary concern has been expressed by certain agencies as to how soon they would have to install such safeguards and whether they would be able to function at all after enactment of the bill until they obtained such features in their systems. For some files or systems, it would be appropriate to define stages and goals to achieve the full level of security. Good-faith compliance can be done in a stage process where necessary, but it is expected that there would be a program of steady and consistent efforts to attain the desired standards.

From the available studies, and from the reports of unauthorized access, it is apparent that few Federal data banks and information systems are living up to existing standards. Testimony to the Committee, the National Academy report and others have shown that there are well-known techniques for controlling authorization of people to use data, to monitor inquiries into the data system, to do current monitoring of the level of use of any participant to detect unusual and possibly unauthorized activity, and other audit-trail techniques. These are all available methods of providing security of systems for administrative, technical, and physical purposes. These and many other techniques are what agencies should be expected to apply to their own situations, within the framework of the Commission model guidelines.

Many of the techniques involved in administrative and physical security would apply to tape central records rooms such as the card index of the Civil Service Commission, the manual fingerprint file of the FBI, and the U.S. Army Records Center.

However, computer systems pose special problems because of on-line terminal communications. Therefore, the growth useful standards and procedure could be nourished.

The notice should include a description of changes in existing inter-agency or intergovernmental informational relationships, whether these are pursuant to Executive order, statute, agreement, or custom. This is to afford the Commission, interested groups, and the Congress an opportunity to evaluate the impact of such computerization or changes in information systems on the observance or principles of separation of powers and of federalism including their impact on powers and authority of State and local governments.

It is expected that precise details to be included in such reports may be arranged with the Privacy Commission, pursuant to consideration of logistical and administrative feasibility.

The Committee intends, by requiring the filing of such notices and the Commission review of them, to assure to the extent possible under this Act the promotion of the public policy reflected in the National Academy of Sciences report that: "All aspects of important new record systems should be subject to examination as to their civil liberties implications and as to citizen reaction to their various features. As with computerization itself, the process of establishing new record systems or changing old ones in executive agencies ought to become more visible and deliberate * * *" (*Report*, p. 399).

Subsection 201(f)(2). Provides that the agency must delay the proposal for 60 days if the Commission, after reviewing the agency's notice and investigating its implications under the terms of the Act and the mandate to the agency under subsection 201(b)(6), as discussed above, notifies the agency that the proposal does not comply with the standards for privacy, confidentiality, and system security established under the Act or by regulation pursuant to it.

This allows the Commission time to file any investigative reports on the matter as required pursuant to title I. Nothing in this Act then prevents agency officials from proceeding with this proposal, nor, on the other hand, does anything in the Act require them to proceed with it. This subsection merely provides for a moratorium of 60 days where the Commission, under its mandate, finds a proposal so fraught with actual or potential constitutional, legal, or administrative difficulties that it ought to be specifically examined or authorized by Congress, or ought to receive the further attention of appropriate high level executive branch officials.

Subsection 201(g). Provides that each Federal agency covered by this Act which maintains a personal information system or file shall make reasonable efforts to serve advance notice on the subject of information before it disseminates or makes available a file or any data on that person pursuant to compulsory legal process. The purpose of this section is to permit an individual advance notice so that he may take appropriate legal steps to suppress a subpoena for his personal data. When it undertakes itself to notify the individual, it may require that the cost burden of such efforts must be borne by the requesting agency or person.

The committee intends subsection (g) to impose stricter requirements upon the disclosure of information to protect it from the searches of random investigators who may obtain information from friendly employees or who may simply flash a badge or use influence to obtain such information. However, the subsection is not intended to require compulsory legal process where it is not presently required. Nor is it intended to loosen any present restrictions imposed by statute or regulation whereby information may only be obtained through court order or other legal process. This subsection reflects the Committee's agreement with the HEW report recommendation which was found necessary "to assure that an individual will know that data are being sought by subpena, summons, or other compulsory legal process, so as to enable the person to assert whatever rights are available to prevent disclosure of the data if such actions seem desirable.

This section is intended to apply to all personal information held by an agency, including administrative, statistical and research data. It is intended to be a separate safeguard independent of any other exemptions in the Act in order to carry out the principle that an individual should be put on notice whenever any agency official is under judicial compulsion to surrender data, and to know whenever personal data will be put to uses unknown to the individual and not specified by the agency in its published notices. In summary, it is designed to assure that the person will be able to exercise rights under this Act to check the data for accuracy or to monitor its further use and redisclosure by the requesting agency or person. Since it is not intended to subtract from existing legal safeguards covering such information demands, it is also intended to allow the individual to exercise any existing rights under Federal and State laws and regulations to challenge the issuance of administrative or judicial orders.

Subsection 201(h). Provides that no person may condition the granting or withholding of any right, privilege, or benefit, or make as a condition of employment the securing by any individual of any information which may be obtained through the exercise of any right secured under the provisions of section 201. It reflects the committee's intention to protect the data subject from coercion by Government agencies or private businesses and organizations who may condition rights, privileges, benefits or considerations otherwise due the person equally with all other citizens upon the obtaining of a personal file or data. This subsection reflects the concerns of administration and agency spokesmen who feared that opening up the individual's personal files which have been protected from disclosure to that person or to others in society would subject the person to all kinds of demands for medical and other personal records. Since the committee's intent is to make certain inroads into the well-meaning paternalism of Federal agencies so that an individual may be advised what information the agency is collecting or holding, this subsection provides a right against such coercion which is enforceable in the Federal District Court in a civil action pursuant to section 303(c). This subsection is not intended to prevent an individual from seeking and obtaining rights under section 201, but is designed to provide a legal remedy for what are believed to be unreasonable and coercive pressures on that person sufficient to state a cause of action before a Federal judge.

Section 202

DISCLOSURE OF INFORMATION

Subsection 202(a). Provides that no Federal agency shall disclose, transfer or disseminate personal files and information to any person, agency or private organization unless certain conditions are met. In conjunction with subsection 201(a)(3), this section is intended to promote the informed consent of the individual to the uses to which government puts the personal data it collects or creates. It is thus expected to exert some check on excessive or illegal reach of governmental power over the individual, and on illegal or inadvertent centralization of investigative programs and linkage of data Federal banks with those in the State and local governments and the private sector. By allowing the individual to know where the data is flowing, the provision should also assist in preventing the illegal or improper use of data by agency officials and employees who have no business with the file or information.

Subsection 202(a)(1). Requires the agency to make written request to the individual and obtain his or her written consent. Compliance with this safeguard may be at the time of initial collection.

Subsection 202(a)(2). Requires the agency to make no such dissemination unless the recipient of the information has adopted rules in conformity with the Act for maintaining the security of its information systems and files and the confidentiality of the information. This mandate, similar to recommendations of several reports and commentators, is to assure continuance upon transfer to another agency or to a governmental or private organization for a Federal purpose, of the protection to which the information is entitled because of the original understanding with the citizen or the originating agency or organization. It is intended to apply to transfer of a particular file of any individual as well as to the transfer of mass data from one automated information system to another, and to the linkage of information systems. If the formal or informal security procedures of the receiving agency clearly or impliedly would allow the data to be used in ways not intended by the individual and not advanced by the agency in its dealings with the person, then no transfer could be made. This would also apply to intergovernmental data-sharing such as transfer of internal revenue files to State and local governments without assuring proper protection for the confidentiality of the data.

While the original bill and the HEW Report envisioned an agency's determining "substantial" assurance of observance by the other agency of such protections, the Committee was told by computer experts and agency representatives that it would be difficult for one agency to enforce such conditions within another agency. Thus, the subsection requires the agency to look to published rules for its judgment on the wisdom of transfer, but anticipates that compliance with the subsection would usually result in creation of interagency negotiations and a record of formal agreement for the conditions of transfer and for protection of the data in the receiving agency.

Subsection 202(a)(3). Prohibits dissemination unless the information is to be used only for the purposes set forth by the sender or by the recipient pursuant to the requirements for notice under subsection

201(c). Again, the same considerations of enforcement and privacy guarantees applicable to the previous subsection apply to this one. The agency transferring is expected, at the minimum, to protect the individual and the public interest by assuring that the uses for which the new agency or user states that it wishes the data are consistent with those for which formal notice has been given by either the transferring agency or the receiving agency or user. Additional guarantees beyond those of this section may be pursued, and, indeed, are encouraged. The Committee recognizes that some agencies take such further precautions as a matter of course for transfer of personal information. This is particularly true of data transferred pursuant to the Federal personnel security program and Executive orders dealing with classified information. Nothing in this section is intended to reduce the strength of those administrative protections for guarantees of privacy and confidentiality.

Executive branch spokesmen and others have advocated that these conditions for interagency and other types of disclosure should be in the alternative. They believe that mere consent of the individual may be enough, or that notice to the public at large of the agency's intended use, or mere requirement of administrative and technical protections for the information, would each alone be sufficient as the general rule governing transfer of personal data. The Committee has disagreed with this approach in the belief that there may be an aura of compulsion or possible threat of intimidation, or an apparent unfair inducement of the individual attached to a request or requirement to surrender personal information for one governmental purpose. This may amount to improper Federal pressure to consent to any and all uses to which the agency may put the data, including that attendant upon interagency or intergovernmental transfer. The best way of guarding against this kind of implicit governmental pressure and affording the individual adequate protection is to require all three conditions. In addition, this prevents an agency from merely citing a notice of intended "use" as a routine and easy means of justifying transfer or release of information. Administration spokesmen were concerned that this might expand interagency data-swapping. By allowing the agency to cite a "use" disclosed by its published notice, the bill is not intended to broaden dissemination and interagency transfer where they must be pursuant to or are required or limited by over 150 Federal statutes. Since subsection 201(a) requires that personal information collected or maintained by the agency be relevant to a statutory purpose, the notice of use and purpose filed with the Commission for the particular information system or data bank will, of necessity, incorporate those statutory uses, and reliance on that notice for transfer authority would represent compliance with subsection 202(a)(3).

The Committee therefore recognizes the great variety of uncoordinated ad hoc, and sometimes poorly authorized patterns of data transfer among agencies. This section does not require such transfers and sharing among agencies, nor does it preclude the additional requirement of other guarantees for safeguarding the individual as well as the originating agency. It is designed to assure, in the future, that one government agency does not use the personal information given by the individual or by third parties to another agency to make what might be a detrimental decision affecting qualifications, rights, bene-

fits, privileges or status, without provision for notice of the existence of the information and obtaining consent, thereby allowing an opportunity to challenge its accuracy and reliability.

Where the information to be transferred to another agency was obtained by compulsion through criminal or civil laws, the safeguards of this section seem particularly necessary in some cases in order to protect the individual's rights under the 5th amendment to due process in the administrative process and before the courts.

Where the disclosure, transfer or dissemination cannot be made due to noncompliance with these standards, there is nothing preventing the requesting agency or the potential user from using whatever legal authority it has to obtain the information from the individual in its own right.

The Securities and Exchange Commission and several regulatory agencies objected to this section under the impression that it would prevent them from obtaining and publishing information which they are required to obtain from people and to publish for the protection of the public. To correct this impression, the Committee adopted an amendment to section 205 as subsection (b) to provide that nothing in the Act shall be construed to permit the withholding by an agency or individual of any personal information which is otherwise required to be disclosed by law or by regulation adopted pursuant to such law.

Disclosure Exceptions

Subsection 202(b), (c), (d), (e) and (f). Establish certain exceptions to these disclosure safeguards on the recommendation of agency and other administration spokesmen that they would otherwise be unworkable or unfair in certain situations, or that they are not necessary in view of other statutory guarantees.

Subsection 202(b)(1). Provides that the notice and consent requirements of subsection 202(a) and the accounting of disclosures and accesses of subsection 201(b)(4) are not applicable when the disclosure would be to officers and employees of the agency who have a need for the information in the ordinary course of the performance of their duties. Determinations of such employees and of their assignments would be consistent with those designated in the list to be kept by the agency under subsection 201(b)(3) for purposes of accounting of access to information. This provision is included to prevent the logistics involved in compliance with the subsection from impeding the day-to-day internal operation of the agency and its offices throughout the country.

Subsection 202(b)(2). Provides that these same subsections do not apply to the Bureau of the Census and its officers and employees when the purpose of the disclosure or transfer is for the purpose of planning or carrying out a census or survey pursuant to the provisions of title 13, United States Code, containing the statutes governing census surveys. Those laws prohibit publication of data gathered by the Bureau in identifiable form and strictly govern confidentiality.

Subsection 202(b)(3). Provides that those two subsections do not apply when the agency determines that the recipient agency has provided advance adequate written assurance that the information will be used solely as a statistical research or reporting record, and is to be transferred in a form that is not individually identifiable. This does not

mean that administrative data in their identifiable form which may be intended for statistical research and reporting uses in the agency or elsewhere is exempt from the requirements of this section or of the rest of the Act.

Pending additional hearings, the Committee has not attempted to deal with all of the reported possibilities of improper or illegal disclosure and use of statistical data when they still have identifiable characteristics or may be linked to the individual.

However, the Committee found no reason why such statistical research or reporting data should not be subject to the appropriate requirements of confidentiality and security in the receiving agency as they were in the sending agency; nor was there reason for exempting such transfer from the requirement that the agency should determine that the information will be used for the purpose set forth in public notice.

Subsection 202(b)(4). This subsection is designed to protect an employee or agency from being in technical violation of the law when they disclose personal information about a person to save the life or protect the safety of that individual in a unique emergency situation. The subsection requires a showing, which should be documented, of compelling circumstances affecting the health or safety of the person, or enabling identification for purposes of aiding a doctor to save such person's life. The discretion authorized here is intended to be used rarely and a precise record of the reasons for the disclosures must be made, including a description of the actions taken to notify the individual at the last known address.

Subsection 202(c). Provides that the prohibitions on disclosure in this section and the requirement in subsection 201(b)(4) of an accounting of the disclosure do not apply when the disclosure would be required or permitted by the Freedom of Information Act of 1966. This provision was included to meet the objections of press and media representatives that the statutory right of access to public records and the right to disclosure of government information might be defeated if such restrictions were to be placed on the public and press. The Committee believed it would be unreasonable and contrary to the spirit of the Freedom of Information Act to attempt to keep an accounting of the nature and purpose of access and disclosures involving the press and public or to impose guarantees of security and confidentiality on the data they acquire.

While the Committee intends in this legislation to implement the guarantees of individual privacy, it also intends to make available to the press and public all possible information concerning the operations of the Federal Government in order to prevent secret data banks and unauthorized investigative programs on Americans.

The Committee does not intend agencies to use the Freedom of Information Act as an excuse to avoid their obligations under this section to obtain informed consent and to assure to the extent possible the lawful use and proper treatment of information transferred to other agencies when it may be used to make a decision about the individual.

Subsection 202(d). Assures that any access to information which the General Accounting Office employees may obtain or any disclosures made to them in the course of their duties which are presently

afforded under existing laws and practices will not be affected by any provisions of this Act. It assures that the General Accounting Office as an arm of Congress will be able to continue to meet its information needs for auditing and inspecting agency programs as required by the Budgeting and Accounting Act and other statutes. This subsection therefore provides that the accounting of access and disclosure required in subsection 201(b)(4) and the conditions which subsection 202(a) attaches to disclosure to other persons and to inter-agency transfer shall not be applied when disclosure would be to the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office. It affirms that nothing in this Act shall impair access by the Comptroller General or his representatives to records maintained by an agency, including records of personal information, in the course of performance of their duties. This subsection reflects the advice of the Comptroller General that such a provision is needed to protect the existing powers which he exercises on behalf of Congress, but that it will not enhance or detract from such powers.

Subsection 202(e). This subsection is designed to provide a general guide for construing the duty imposed on agencies by this section and those imposed by the Federal Reports Act and other statutes to promote efficiency and economy by combining data requests and sharing the results and thus reduce repetitive demands on citizens. It is to reflect the Committee's intent that the requirements of this section are to be interpreted as a mandate to continue enforcement of the duties imposed by other statutes, and that they should not prevent agencies from taking whatever management steps are needed to implement the two goals in drafting their questionnaires and in planning and carrying out their information programs. In addition, it has been included to meet the concerns of Administration spokesmen that the minimum safeguards for interagency disclosure under this section might be interpreted by agencies as an indication that they could relax their efforts to comply with the present restrictions placed on some exchanges of information between agencies for the purpose of promoting confidentiality of certain kinds of records.

The Committee believes that there are a number of administrative devices for assuring observance of the two sets of values in Federal information programs, but we have not attempted to close all of the administrative loopholes which allow violation of confidentiality.

Subsection 202(f). Provides an exemption from the written request to the individual prerequisite for disclosure with respect to requests by law enforcement agencies. Obv ously it would be inappropriate to require a law enforcement agency to get permission of the subject of a criminal history record prior to obtaining a copy from another law enforcement agency. Such a requirement would in effect prohibit the routine exchange of records through the FBI's Identification Division or the National Crime Information Center (NCIC). Likewise, it might frustrate legitimate criminal investigations if a law enforcement agency were required to get permission from the subject of a file maintained by a non-law enforcement agency before the former agency could gain access. (e.g. FBI access to a tax return).

Subsection 202(f). Recognizes both types of law enforcement, disclosure, or access to files by distinguishing between routine and non-routine exchanges of information with law enforcement agencies. The Committee assumes that most routine exchanges with law enforcement agencies involve law enforcement records such as rap sheets or criminal histories and is between two law enforcement agencies; and that the less routine disclosure to a law enforcement agency involves a law enforcement agency request of a non-law enforcement agency. Therefore subsection (e) permits law enforcement disclosure in the former circumstance, where there is a program of routine exchange, if there is a formal agreement between the two agencies respecting such exchange. The subsection permits law enforcement access in the second circumstance, non-routine requests only where written requests and permission are given on a case-by-case basis by the agency maintaining the record. The Committee is of the view that the agency which maintains the records should assure, via the written permission or the formal agreement that the recipient has complied with subsection 202(a)(2) and adopted rules on security, confidentiality, and privacy.

If the exchange is on a routine basis, the two agencies should adopt a formal agreement between themselves setting out which records will be exchanged, how the records may be used and the privacy, confidentiality, and security regulations which the recipient agency has adopted. The sanction for failure to comply with the agreement should be interruption of routine exchange by the maintaining agency. This formal agreement concept is based upon the terminal users agreement now used by NCIC and by state and local law enforcement agencies which operate data banks. The Commission and the Attorney General would, of course, have to determine whether an existing terminal agreement adequately meets the requirements of this subsection once this bill is enacted and how that concept will be applied to manual files. Any such agreements would in effect be public documents since they would be incorporated into the public notice given on the information systems as required by subsection 201(c).

Although the Committee believes that public notice and exposure of such routine exchange will act as a check on abuses of such arrangements, the committee hopes that routine exchange will be restricted to essential law enforcement records such as rap sheets and that those records will only be exchanged by such agreement between law enforcement agencies. All other types of access should be via the written request according to the agency procedure. In requiring that the agency rule on each request on a case-by-case basis, it is hoped that secret law enforcement access, that is disclosure without notification to the subject of the file, will only be permitted in the most exigent and essential circumstances. In each such case, the agency must find that such circumstances exist and that the law enforcement agency has described the information requested in sufficient particularly to meet the requirements of the subsection. The subsection specifically requires that the law enforcement agency set out in its written request of the agency "the particular portion of the information desired and the law enforcement activity for which the information is sought."

Section 203

EXEMPTIONS

Subsection 203(a). The Committee believes that it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency. The existence and certain characteristics of each system should be a matter of public record, and testimony before the Committee has indicated that this information can be made public without compromising critical information used by agencies responsible for the national defense or foreign policy of the country.

The potential for serious damage to the national defense or foreign policy could arise if the notice describing any information system included categories or sources of information required by subsection 201(c)(3)(E) or provided individuals access to files maintained about them as required by subsection 201(d).

The Committee does not by this legislation intend to jeopardize the collection of intelligence information related to national defense or foreign policy, or open to inspection information classified pursuant to Executive Order 11652 to persons who do not have an appropriate security clearance or need to know.

This section is not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information. Many personnel files and other systems may not be subject to security classification or may not cause damage to the national defense or foreign policy simply by permitting the subjects of such files to inspect them and seek changes in their contents under this Act. In order to obtain an exemption from subsection 201(c)(3)(E) or 201(d), it must be shown that the application of those subsections would damage or impede the purpose for which the information is maintained.

Subsection 203(b). Exempts from full compliance with the access and challenge provisions of section 201 and the disclosure provisions of section 202, that information which an agency head determines is investigative information or law enforcement intelligence information. Both terms are precisely defined in the definitions section of the bill contained in Title III. All of these definitions are based in large part on the criminal justice privacy bills (S. 2963 and S. 2964) discussed earlier in the section of the report dealing with law enforcement.

The effect of this subsection is to require the agency head to determine first what portion of files maintained in any information system in his agency or which his agency might fund on the State or local level contains information which falls within the definitions—"Investigative information" or "law enforcement intelligence information." Investigative information might include information in a file maintained by a legitimate law enforcement agency, defined as an agency which can make an arrest for violation of a Federal or State statute. Investigative information might also be maintained by an agency which is not a law enforcement agency but which is gathering the information in the course of investigating activity which falls within its regulatory jurisdiction. For example, this section would permit the Chairman of the SEC to exempt from access and challenge files maintained by his agency on individuals whom it is investigating for violation of the SEC laws.

The exemption for intelligence information is restricted for the most part to law enforcement agencies. It was the Committee's view that there were no regulatory or non-law enforcement agencies which had a legitimate right to maintain intelligence files and that therefore none of their investigative files should be exempt from the access, challenge and disclosure provisions via reliance on exemptions for intelligence information.

Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained". The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information (e.g. all wiretap transcripts maintained at FBI) and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.

The subsection 203 (b) qualifies the exemption from access and disclosure for investigative information in two important respects. First, investigative information may not be exempted under this section where the information is maintained longer than is necessary to commence criminal prosecution. This qualification recognizes the amendments to the Freedom of Information Act recently adopted by the Senate (the so-called Hart amendment). Second, the subsection states that the Act is not intended to disturb the rules of criminal and civil discovery of investigative files presently permitted by the Federal Rules of Criminal and Civil Discovery and, other State or Federal court rules, administrative regulations or statutes such as the so-called "Jencks" statute (18 USC 3500).

Subsection 203 (c)(1). The head of any agency may determine that an information system file or personal information maintained by that agency qualifies for an exemption under subsection (a) or (b) of this section. To secure the exemption, a notice of proposed rule-making must be published in the Federal Register at least 30 days prior to holding rule-making proceedings and provide a copy of that notice to the Privacy Protection Commission to afford the Commission the opportunity to comment. Where possible, agencies are encouraged to provide up to 60 days' notice of hearings to afford all interested parties an opportunity to comment or appear.

The notice of the proposed rule-making shall conform to the requirements of sections 553(b), (c) and (e); 556, and 557 of Title 5, United States Code and shall include a specification of the nature and purpose of the system file or information to be exempted as provided by subsection 201(c) of this Act.

After the period of notice, the agency shall give interested persons an opportunity to participate in the rule-making through submission of written arguments or through oral presentation at a public hearing.

After consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose.

Section 204

ARCHIVAL RECORDS

Subsection 204(a). Provides for certain applications of the Act to archival records. Federal agency records which are deposited and accepted by the Administrator of General Services for storage, processing and servicing in accordance with section 3103 of title 44 of the United States Code are to be considered as though maintained by the agency which deposited the records and subject to all of the provisions of this Act, where they apply to such agency records. The Administrator of General Services is prohibited from disclosing such records or any information in them, except to the agency which maintains the records or pursuant to the rules established by that agency.

Subsection 204(b). Provides that Federal agency records pertaining to identifiable individuals which were transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the Federal Government are to be considered to be maintained by the National Archives for the purposes of this Act. Except for the required annual public notice set forth in subsection 201(c), the only provisions for the act which shall apply to such records are subsections 201(b)(5), requiring the establishment of rules of conduct and appropriate training for employees and 201(b)(6), requiring the establishment of appropriate administrative, technical and physical safeguards to protect the confidentiality of personal information. These provisions are, to a large extent, already a part of existing rules of the National Archives and hence should pose no unwarranted administrative burden.The Committee finds no reason why the Administrator should not establish rules of conduct and notify the employees and others involved in any phase of the information system or file of the requirements of the Act concerning the need for respect for the needs of privacy, confidentiality and for security of the system. In addition, there is no valid reason why the Archives should be exempt from the requirement to establish the appropriate safeguards to insure the security of the system.

Along with all other agencies, the National Archives is subject to the notice requirements of the bill.

Subsection 204(c). Provides that the National Archives shall notify the Commission and give public notice of the existence and character of the personal information systems and files which it maintains for its own internal uses and for other purposes and cause such notice to be published in the Federal Register. While it realizes the difficulties of describing these precisely, the Committee intends such notice to include at least the information specified by subsection 201(c)(3) (G), (I) and (J).

The Administrator of the General Services Administration testified against application of the bill to records under GSA control or to those in the National Archives. This is particularly true of the Archives

63-619 O - 76 - 16

records which are generally over 50 years old and are not well organized. The Committee consulted with GSA staff and has learned that records at the Archives are inadequately indexed and involve large volumes of data in more than 20,000 separate filing systems; hence the Committee believes that the administrative cost of compliance by the Archives would far outweigh any potential benefits, particularly since records cannot be disclosed by the Archives unless they are at least 50 years old. However, the Committee intends that the Administrator of General Services take special precautions to ensure that records older than 50 years not be disclosed when disclosure is likely to cause discreditation or injury to an elderly individual or the living relatives of deceased individuals. In the case of Bureau of the Census records assembled subsequent to the year 1900, disclosure ought to be subject to the approval of the Secretary of Commerce.

The Committee believes that this section adequately meets the problems he described in his testimony. It is designed to further the interest of historians and others in preserving the integrity of historical records and in promoting access to them, within the constraints of the needs for individual privacy, for confidentiality and due process of law.

Section 205

exceptions

Section 205 provides certain general exceptions and clarifies legislative intent.

Subsection 205(a). Shows the Committee's intent that the exemptions provided in the Freedom of Information Act to the required disclosure of Federal information on certain subjects, and that permitted for protection of personal privacy may not be used as authority to deny an individual personal information otherwise available under this Act.

Subsection 205(b). Reflects the Committee's intent that the Act does not affect existing requirements to disclose, disseminate, or publish information which an agency is required to collect for the purpose of making such disclosure. This subsection was included at the request of the Securities and Exchange Commission and other regulatory agencies to assure that this Act will not affect their statutory duties to publish information.

Subsection 205(c). Exempts from the access and challenge provisions information collected, furnished or used by the Census Bureau for statistical purposes or as authorized by the Federal Census statutes. While statistical records are subject to other safeguards and requirements of the Act, the Committee believes that the complex statutory and administrative scheme presently governing census and statistical information needs careful legislative review before attempting to apply the provisions for access, challenge and review of such records. The Director of the Census Bureau referred to the millions of statistical records now in existence and the very specific procedures and rigorous safeguards applied to them. The Census Bureau records are not used to make decisions about individuals but are used to furnish to those individuals extracts of otherwise confidential information about themselves, and their immediate families.

Section 206

MAILING LISTS

Subsection 206(a). Prohibits, unless specifically authorized by law, the practice by Federal departments and agencies of selling or renting names and addresses which they acquire during their transactions with individuals or which they obtain through their dealings with other agencies. The Committee believes this provision is consistent with the intent of the bill to prevent disclosures of personal information without consent or specific authority. As discussed in this report the clear difficulty in obtaining consent free of the appearance of intimidation and the impossibility of assuring limited use once the data is sold or rented, makes it advisable to require specific approval by Congress when the agency undertakes to sell or rent this data in bulk.

This stipulation should not be construed to require an agency to withhold from the public names and addresses which are otherwise permitted to be made public.

The provision is not intended to affect the protection already afforded and the authorized uses now designated for the names and addresses of individual postal customers maintained by the Postal Service to facilitate mail delivery, mail forwarding, and address and mailing list correction services. Present law prohibits the Postal Service from making available to the public any mailing or other list of names and addresses, except as specifically provided by law.

Subsection 206(b). Deals with the disclosure and use of names and addresses by any person, including businesses and organizations, engaged in interstate commerce, who maintains a mailing list. It requires removal of the individual's name and address from such list, upon written request of that individual. The bill thus provides a right to individuals which heretofore has been granted by some organizations, and which has been recognized by the Direct Mail Marketing Association as a desirable standard for organizations which use mailing lists. This provision does not attempt to regulate the maintenance of files and personal records of State and local governments, or of organizations or their use of names and address for communicating with customers, clients and others with whom they have commercial transactions or official business.

TITLE III—MISCELLANEOUS

Section 301

DEFINITIONS

Section 301 contains the definitions applicable to the bill.

The Committee has used the term "*personal information*" throughout the bill to mean any information about the individual that identifies or describes any characteristic including but not limited to education, financial transactions, medical history, criminal or employment record, or any personal information that affords a basis for inferring personal characteristics such as finger and voice prints, photographs, or things done by or to such individual. Such definition

includes the record or present registration, or membership in an organization or activity, or admission to an institution. It is intended to include within these terms any symbol, number, such as a social security number or character, address, by which the individual is indexed in a file or retrievable from it.

The reference to personal characteristics does not exclude a file that contains only names and is headed by a general label for a category of records. If the heading or the nature of the file represents a judgment on the individual or a subjective view, then that file would be subject to the bill. A file headed "security risks" or one labeled "malingerers," or one coded for people to be dismissed at the earliest opportunity, even if the file only contained names, would be covered. This could, for instance, include a list of people who do not buy bonds, or do not contribute to charitable causes. Thus it could cover a list which contained names only but which, by its nature, conveyed something detrimental or threatening to the reputation, rights, benefits or privileges or qualification of the individual simply by reason of being listed on it. There are many data banks and files with names maintained strictly for housekeeping purposes, and it is expected that the Commission model guidelines will make some distinctions for the degrees of sensitivity of such files, and will allow for the development of special treatment for files where the potential for abuse and harm is very great, and those for housekeeping purposes such as who works on a holiday or who has a parking space.

The term "*individual*" means a citizen of the United States or an alien lawfully admitted through permanent residence. This term is used instead of the term "person" throughout the bill in order to distinguish between the rights which are given to the citizen as an individual under this Act and the rights of proprietorships, businesses and corporations which are not intended to be covered by this Act. This distinction was to insure that the bill leaves untouched the Federal Government's information activities for such purposes as economic regulations. This definition was also included to exempt the coverage of the bill intelligence files and data banks devoted solely to foreign nationals or maintained by the State Department, the Central Intelligence Agency and other agencies for the purpose of dealing with nonresident aliens and people in other countries.

The term "*information system*" was adopted to indicate the application of the bill to all of the components and operations, whether automated or manual or otherwise maintained, by which personal information, including the name or identifier, is collected, stored, processed, handled or disseminated by an agency.

Rather than focus on a single record or subject file, the Committee has adopted an approach focused on the total information system which includes all phases of information collection, storage, handling, processing, dessimination and transfer. It includes records which are computerized, mechanized, microfilmed and photographed. The bill thus is directed to the overall programs and policies of executive branch departments and agencies including the design, development, and management of an information system, as well as to the maintenance of one particular file on an individual, or the gathering of information on one data subject. With such a definition, the duties and responsibilities imposed by the bill apply to administrators, computer

programmers and all manner of employees including technicians, clerks, guards. Given the broad scope of the bill, an alternative use of the term "system of record" would create confusion as to its possible application to such things as inventories and extraneous matters.

The use of the terms "information system" and "files" allows for distinctions where needed for the application of certain standards to an entire information system of an agency, department, or establishment, including its bureaus, offices, employees, and equipment, and for the application of them to a particular file, that is, a series of records, on a particular subject.

The terms "*file*" and "*data bank*" in public usage are frequently interchangeable.

Under this bill, "file" may mean an individual record or a series of records containing personal information about individuals which may be maintained within an information system. "Data bank" means a collection of files pertaining to individuals. Used in the bill, it connotes a recognizable entity for management purposes, specifically located within an agency or organization or to one of its components; it means a collection of files usually contributed to by different users and available to them according to a plan of access.

The term "*Federal agency*" means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States. The definition includes any officer or employee of an agency. In addition to the general purpose of this provision to define the application of the Act, it is also intended that the definition assist in placing the responsibility for intra-agency handling of information on the head of the department or agency.

The term "*investigative information*" has a special and narrow meaning under this bill. It has been discussed at length in the section of the report entitled "Law Enforcement Files". It means information associated with an identifiable individual compiled by—

(1) an agency in the course of conducting a criminal investigation of a specific criminal act where such investigation is pursuant to a statutory function of the agency. Such information may pertain to that criminal act and be derived from reports of informants and investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically and expressly required by State or Federal statute to be made public; and

(2) by an agency with regulatory jurisdiction which is not a law enforcement agency in the course of conducting an investigation of specific activity which falls within the agency's regulatory jurisdiction. For the purposes of this paragraph, an "agency with regulatory jurisdiction" is an agency which is empowered to enforce any Federal statute or regulation, the violation of which subjects the violator to criminal or civil penalties.

The term "*law enforcement intelligence information*" means information associated with an identifiable individual compiled by a law enforcement agency in the course of conducting an investigation of an individual in anticipation that he may commit a specific criminal act,

including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically by incident and expressly required by State or Federal statute to be made public.

The term *"criminal history information"* means information on an individual consisting of notations of arrests, detentions, indictments, informations, or other formal criminal charges and any disposition arising from those arrests, detentions, indictments, informations, or charges. The term shall not include an original book of entry or police blotter maintained by a law enforcement agency at the place of an original arrest or place of detention, indexed chronologically and required to be made public, nor shall it include court records of public criminal proceedings indexed chronologically.

The term *"law enforcement agency"* means an agency whose employees or agents are empowered by State or Federal law to make arrests for violations of State or Federal law.

Section 302

CRIMINAL PENALTY

Section 302 provides for criminal penalties for willful violations of the Act in two respects. One is for the secret creation of data banks in violation of the requirement that all such decisions be made public. Any officer or employee of any Federal agency who willfully keeps an information system without meeting the notice requirements of this Act set forth in subsection 201(c) shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

The other violation subjects an officer or employee of the Commission to criminal penalty for the unlawful disclosure or transfer of personal information about any individual obtained in the course of such officer or employee's duties in any manner or for any purpose not specifically authorized by law and provides that such person be fined not more than $10,000 or imprisoned not more than five years, or both.

These are the only violations of the Act subject to criminal sanction. The Committee has decided to provide criminal sanctions for these two violations because they are key to any effective protection for privacy and confidentiality. The public policy requires that all data banks be subject to a visible public policy decision. The entire Act would be frustrated if secret data banks could be created and operated with impunity. The Committee has underlined this judgment by not permitting an exclusion from this requirement even for those highly sensitive data banks in the areas of national defense, foreign policy or law enforcement. A strongly-enforced requirement of publicity in the creation of data banks is necessary for administrative oversight, legislative oversight, and judicial review.

Equally fundamental is the need to guard against unlawful dissemination, disclosure or transfers of personal information acquired by the Commission consultants and employees in the course of their duties.

While Commission employees are also subject to the same Federal criminal laws and government-wide regulations penalizing all other Federal employees who disclose information, this section creates sanctions uniquely applicable to them. This is deemed necessary since in exercise of its powers and performance of investigative duties, the Commission may obtain or examine all kinds of administrative documents and data relative to executive branch implementation and enforcement of the Act, as well as information on individuals needed to determine violations of the Act. In addition, for purposes of its research and studies, it may engage in similar activities with respect to certain data banks and systems of the private sector and in State and local governments.

In light of such special auditing, inspection and study functions, strong penalties were deemed necessary to reassure government agencies and citizens that the deterrents to improper disclosure are so severe that they need not worry about improper or illegal disclosures.

Section 303

CIVIL REMEDIES

Section 303 provides for civil judicial enforcement of the Act by persons affected by violations of the Act. In keeping with general legislative practice, this bill not only establishes certain administrative requirements and grants certain rights to citizens, but gives authority to the citizen to defend his rights by taking the initiative of court action. Such a right is doubly important since the revised bill gives no enforcement authority to the Commission.

Subsection 303(a). Gives a cause of action to a citizen aggrieved by a denial of access to his own file. Since access to a file is the key to insuring the citizen's right of accuracy, completeness, and relevancy, a denial of access affords the citizen the right to raise these issues in court. This would be the means by which a citizen could challenge any exemption from the requirements of sections 201 and 202 made pursuant to the procedures outlined in section 203. A person seeking access to a file which he has reason to believe is being maintained on him for the purposes of determining its accuracy and completeness, for example, or to take advantage of the rights afforded him under section 201, could raise the question of the propriety of the exemption which denies him access to his files. In deciding whether the citizen has a right to see his file or to learn whether the agency has a file on him, the court would of necessity have to decide the legitimacy of the agency's reasons for the denial of access, or refusal of an answer. The Committee intends that any citizen who is denied a right of access under the Act may have a cause of action, without the necessity of having to show that a decision has been made on the basis of it, and without having to show some further injury, such as loss of job or other benefit, that might stem from the denial of access. Since it is often exceedingly difficult for a citizen to learn of such consequences, or if he knows, to establish a "cause and effect" relationship between the information in his file and some subsequent damage to him, the Committee has decided that it would frustrate an individual's ability to assert his rights if he had to allege and prove use or such consequential harm. In order to state a cause of action, it should be enough that he be able to assert that the presumptive right of access granted him by the Act has been denied him.

Subsection 303(b). Affords the Attorney General and any aggrieved person authority to enforce the Act as against existing or threatened violations of the Act by seeking a Federal District Court injunction against such acts or practices. This subsection has a two-fold purpose. First, it gives the Attorney General the obligation to challenge in court any violation of the Act which might affect the public at large, but which does not yet affect any particular citizen sufficiently to give him constitutional standing to sue, or which may not be such as to induce a private person to endure the practical difficulties of litigation.

Second, the grant of a cause of action to any "aggrieved person" is designed to encourage the widest possible citizen enforcement through the judicial process. This is necessary, as mentioned, since the Act does not give any administrative body authority to ensure compliance with the Act. The Committee intends the use of the term "aggrieved person" to afford the widest possible standing consistent with the constitutional requirement of "case or controversy" in Article III, Sec. 2 of the Constitution. In this respect, the provision is designed, among other things, to supply certain deficiencies in standing and ripeness which the courts found in the *Environmental Protection Agency* v. *Mink*, 410 U.S. 73 (1973), *Laird* v. *Tatum* (408 U.S. 1(1972), and *Stark* v. *Schultz*, 42 U.S.L.W. 4481 (Apr. 1, 1974)).

Subsection 303(c). Provides that any person found to have violated provisions of the Act or any rule, regulation, or order issued under it shall be liable to the aggrieved person for actual damages sustained by the individual, punitive damages where appropriate, and in case of successful action, the cost of the action, with reasonable attorney's fees to be determined by the court.

In addition to damages, the aggrieved person would receive the benefit of any other appropriate remedies, including injunctive or mandatory relief, which the court deems appropriate.

The final subsection makes clear that the Federal courts will have jurisdiction regardless of the fact that the amount claimed is less than $10,000.

Section 304

jurisdiction of district courts

Subsection 304(a). Gives jurisdiction to the Federal courts to hear cases brought under section 303 and to examine information *in camera* to determine whether the information or any part of it may be withheld under any of the exemptions in section 203 of the Act. The agency has the burden of sustaining the legality of its actions. Venue would most likely be either in the plaintiff's jurisdiction, or in Washington, D.C., although other venue is possible. The section also ensures that the court will have the power to examine *in camera* any contested information necessary to a determination of the litigation, thus among other things, remedying the lack of reviewing power which the Supreme Court found in the *Mink* case. Since the burden of justifying the withholding of information is on the agency, this will enable the court to make a full *de novo* determination of the propriety of the grounds asserted by the government for keeping the information from the plaintiff. Such a provision is necessary in order to provide a full and complete hearing to the issues being litigated and to provide justice to the aggrieved individual.

Subsection 304(b). Provides that in any action to obtain judicial review of a decision to exempt any personal information from any provision of this Act, the Court may examine such information *in camera* to determine if all, or any part of it, is properly classified with respect to national defense, foreign policy, or law enforcement intelligence or investigative information and may be exempted from any provision of this Act. The burden is on the Federal agency to sustain any claim that such information may be so exempted.

Section 305

EFFECTIVE DATE

Provides that the Act shall become effective one year after the date of enactment, except that the provisions of title I shall become effective on the date of enactment.

This provision is designed to allow the agencies lead time to develop their regulations and to seek such additional resources or assistance as they may need to meet their obligations under the Act. By allowing the immediate implementation of the provisions establishing the Commission, the Committee intends to permit the Commission time to develop its model guidelines, establish any needed interagency councils, and generally to prepare for full implementation of the Act.

Section 306

AUTHORIZATION OF APPROPRIATIONS

Authorizes appropriation of such sums as may be necessary to carry out the provisions of the Act.

New Title

The title is amended so as to read:

"A bill to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes."

Estimated Cost of the Legislation

The Committee has received a broad variety of generalized statements of the estimated costs of implementing the safeguards and guarantees provided in this legislation. No precise estimate of costs can be established until the Commission develops model guidelines and until the Act is applied to specific information programs and administrators have reviewed their resources for implementing it in accordance with their own rules. The Committee believes that good faith enforcement of the standards and procedures for review will result in substantial savings to Federal agencies. We are mindful, for instance, of testimony describing the Navy's destruction of 15 tons of records upon review of its program needs for retention of records. Similar patterns showed up in the review by the Army of the relevance to its statutory programs to the personal information it collected and maintained on individuals who had no dealings with the armed services.

Since a number of agencies already apply some of the safeguards to certain of their files, and since the Act will require little or no further effort on their part for those files, this certainly will affect the cost of implementation. Furthermore, experience under the practices of those agencies and with provisions which are somewhat similar in the Fair Credit Reporting Act and other statutes shows that the workload is not unreasonable and, in some cases under those laws, did not meet expectations. The very existence of the statutory guarantees apparently tended to reassure citizens that government and organizations were following certain guidelines pursuant to administrative and legislative oversight.

The HEW report addressed the problem of costs and the Committee agrees with the commonsense observations there:

> The safeguards we recommend will not be without costs, which will vary from system to system. The personal data record-keeping practices of some organizations already meet many of the standards called for by the safeguards. . . . We believe that the cost to most organizations of changing their customary practices in order to assure adherence to our recommended safeguards will be higher in management attention and psychic energy than in dollars. These costs can be regarded in part as deferred costs that should already have been incurred to protect personal privacy, and in part as insurance against future problems that may result from adverse effects of automated personal data systems. From a practical point of view, we can expect to reap the full advantages of these systems only if active public antipathy to their use is not provoked. (Report, p. 44, 45)

The Office of Management and Budget has been unable to provide an accurate cost estimate.

ROLLCALL VOTE ON FINAL PASSAGE

In compliance with section 133 of the Legislative Reorganization Act of 1946, as amended, rollcall votes taken during Committee consideration of this legislation are as follows:

FINAL PASSAGE: Ordered reported: 9 yeas—0 nays

Yeas:
Jackson
Muskie
Chiles
Nunn
Huddleston
Percy
Roth
Brock
Ervin

(Proxy)
Ribicoff
Javits.

Nays:
None

93D CONGRESS
2D SESSION

H. R. 16373

IN THE HOUSE OF REPRESENTATIVES

AUGUST 12, 1974

Mr. MOORHEAD of Pennsylvania (for himself, Ms. ABZUG, Mr. ALEXANDER, Mr. BROOMFIELD, Mr. ERLENBORN, Mr. FASCELL, Mr. GOLDWATER, Mr. GUDE, Mr. KOCH, Mr. LITTON, Mr. MCCLOSKEY, Mr. MOSS, Mr. THONE, and Mr. WRIGHT) introduced the following bill; which was referred to the Committee on Government Operations

A BILL

To amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Privacy Act of 1974".

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from any collection, maintenance, use, and dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring each Federal agency to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, and disseminated by each such agency;

(2) permit an individual to prevent records pertaining to him obtained by each such agency for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to certain Federal agency records pertaining to him, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or negligent action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the

United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any collection or grouping of data about an individual that is maintained by an agency and that contains his name, identifying number, symbol, or other identifying particular assigned to each such individual;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to each such individual; and

"(6) the term 'statistical research or reporting record' means a record in a system of records assembled or maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13, United States Code.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record to any person, or to another agency, except pursuant to a written request by, or with the prior

written consent of, the individual to whom the record pertains, unless disclosure would be—

"(1) to those officers and employees of that agency who have a need for such record in the performance of their duties;

"(2) required pursuant to section 552 of this title or any other Federal statute;

"(3) for a routine use described in any rule promulgated pursuant to subsection (e) (4);

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey pursuant to the provisions of title 13, United States Code;

"(5) where the agency determines that the recipient of such record has provided advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and is to be transferred in a form that is not individually identifiable;

"(6) when transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity if such activity is authorized by statute and if the head of such agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought; or

"(8) pursuant to a showing of compelling circumstances affecting the health, safety, or identification of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency, except for disclosures made pursuant to subsection (b) (1) through (6); and

"(B) the name and address of the person or agency to whom such disclosure is made;

"(2) retain the accounting made pursuant to paragraph (1) for at least five years after the disclosure for which such accounting is made;

"(3) except for disclosures made pursuant to subsection (b) (7), make the accounting available to the individual named therein at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of any record that has been disclosed to such person or agency within two years preceding the making of such correction of the individual's record, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section and for which there is no accounting of such disclosure.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to any record pertaining to him which is contained in any particular system of records maintained by the agency, permit him to gain access to such record and have a copy made of all or any portion thereof in a form comprehensible to him;

"(2) permit such individual to request amendment of a record pertaining to him and either—

63-619 O - 76 - 17

"(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(B) promptly inform such individual of its refusal to amend such record in accordance with his request, the reason for such refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

"(3) permit any such individual who disagrees with the agency's refusal to amend his record to request review of such refusal by the official named in accordance with paragraph (2) (B); and if, after such review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the agency's refusal; and

"(4) in any disclosure relevant to such individual's disagreement occurring after the filing of the statement under paragraph (3), clearly note any portion of such record which is disputed and provide copies of such statement and, if the agency deems it appropriate, copies of a concise statement of the agency's reasons for

not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed.

"(e) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules in accordance with the requirements, including that of general notice, of section 553 of this title. Such rules shall—

"(1) include a notice of the existence and character of each system of records which the agency maintains, which notice shall consist of—

"(A) the name and location of each such system;

"(B) the categories of individuals on whom records are maintained in such system;

"(C) the categories of information maintained in such system; and

"(D) the title and business address of the agency official or employee who is responsible for such system;

"(2) establish procedures whereby an individual from whom information pertaining to him is being requested is apprised of the general purposes for which such information will be used;

"(3) describe the policies and practices of the

agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(4) describe for each system of records, each routine purpose for which the records contained in such system are used or intended to be used, including the categories of users of the records for each such purpose;

"(5) provide that any record which is used by the agency in making any determination about any individual is maintained with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness to the individual in such determination;

"(6) establish procedures whereby an individual can be notified in response to his request if any particular system of records contains a record pertaining to him;

"(7) define reasonable items, places, and requirements for identifying individuals who request records pertaining to themselves before the agency shall make such records available to such individuals;

"(8) establish procedures for the disclosure to an individual upon his request of records pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(9) establish procedures for reviewing requests from individuals concerning the amendment of records pertaining to such individuals, for making a determina-

tion on such requests, for appeals within the agency of initial adverse agency determinations, and for whatever additional means the head of the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and

"(10) establish fees to be charged, if any, to individuals for making copies of their records, excluding the cost of any search for such records and review of them.

"(f) (1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d) (1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to such individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such records and consequently makes such a determination which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, such individual may bring a civil action against such agency, and the district courts of the United States shall have jurisdiction in such matters as provided by paragraph (4) of this subsection.

"(2) (A) In any suit brought pursuant to the provisions

of subsection (f) (1), the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether such records or any portion thereof may be withheld under any of the exemptions set forth in subsection (i) or (j) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(3) In any suit brought pursuant to the provisions of subsection (f) (1) in which the court determines—

"(A) that the agency's refusal or failure has been willful, the agency shall be liable to the individual in an amount equal to the sum of—

"(i) actual damages sustained by the individual as a result of such refusal or failure;

"(ii) punitive damages allowed by the court; and

"(iii) the costs of the action together with reasonable attorney's fees as determined by the court; or

"(B) that the agency's refusal or failure has been negligent, the agency shall be liable to the individual in an amount equal to the sum of—

"(i) any actual damages sustained by the individual as a result of such refusal or failure; and

"(ii) the costs of the action together with reasonable attorney's fees as determined by the court.

"(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the agency's liability to that individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

"(g) RIGHTS OF LEGAL GUARDIANS.—For the purposes of subsections (b), (d), and (f) of this section, the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age

by a court of competent jurisdiction may act on behalf of such individual.

"(h) (1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information, the disclosure of which is prohibited by this section or by rules or regulations established pursuant thereto, and who knowing that disclosure of such specific material is so prohibited, willfully discloses such material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.

"(i) GENERAL EXEMPTIONS.—Except for subsections (e) (1) and (e) (3), the provisions of this section shall not apply to any record or system of records which is—

"(1) maintained by any agency to the extent that the President determines by Executive order, on an annual basis, that providing access by an individual to his records would cause serious damage to the national defense or foreign policy;

"(2) maintained by the Central Intelligence Agency; or

"(3) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (a) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (b) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (c) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

"(j) SPECIFIC EXEMPTIONS.—Subsections (b), (c)(3), (d), (e)(2), and (e)(6) through (10) shall not apply to any record or system of records which is—

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law en-

forcement purposes, except to the extent that such material is within the scope of paragraph (i) (3) or is open to public inspection under the provisions of section 552 (b) (7) of this title;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18, United States Code;

"(4) investigatory material maintained for the purpose of determining initial or continuing eligibility or qualification for Federal employment, military service, Federal contracts, or access to classified information;

"(5) material used for appointment, employment, or promotion in the Federal service; or

"(6) required by statute to be maintained and used solely as statistical research or reporting records.

"(k) (1) ARCHIVAL RECORDS.—Agency records which are accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44, United States Code, shall, for the purposes of this section, be considered to be maintained by the agency which deposited the records and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose such records, or any information therein, except to the agency which maintains the records or pursuant to rules established by that agency.

"(2) Agency records pertaining to identifiable individuals which were transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section.

"(3) Agency records pertaining to identifiable individuals which are transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsection (c) (4); (d) (2), (3), and (4); (e) (2), (5), and (9); (f) (1) (B) and (C); and (f) (3).

"(l) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section pursuant to the provisions of subsections (i) and (j) of this section during

the preceding calendar year, and the reasons for such exemptions, and such other information as indicates efforts to administer fully this section."

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings."

SEC. 5. (a) Title 44, United States Code, is amended by adding after section 3506 the following new section:

"§ 3506a. Information concerning political and religious beliefs and activities

"No Federal agency shall maintain any record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained."

(b) The chapter analysis of chapter 35 of title 44, United States Code, is amended by inserting:

"3506a. Information concerning political and religious beliefs and activities."

immediately below:

"3506. Determination of necessity for information; hearing."

SEC. 6. The amendments made by this Act shall become effective on the one hundred and eightieth day following the date of enactment of this Act, except that the amendments

made with respect to section 552a(e) of title 5, United States Code, shall become effective on the date of enactment of this Act.

Union Calendar No. 682

93D CONGRESS
2D SESSION

H. R. 16373

[Report No. 93–1416]

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 2, 1974

Mr. MOORHEAD of Pennsylvania (for himself, Ms. ABZUG, Mr. ALEXANDER, Mr. BROOMFIELD, Mr. ERLENBORN, Mr. FASCELL, Mr. GOLDWATER, Mr. GUDE, Mr. KOCH, Mr. LITTON, Mr. MCCLOSKEY, Mr. MOSS, Mr. THONE, and Mr. WRIGHT) introduced the following bill; which was referred to the Committee on Government Operations

OCTOBER 2, 1974

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, ~~That this Act may be cited as the "Privacy Act of 1974".~~

~~SEC. 2. (a) The Congress finds that—~~

~~(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;~~

~~(2) the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from any collection, maintenance, use, and dissemination of personal information;~~

~~(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;~~

~~(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and~~

~~(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.~~

~~(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring each Federal agency to—~~

~~(1) permit an individual to determine what records pertaining to him are collected, maintained, used, and disseminated by each such agency;~~

~~(2) permit an individual to prevent records pertaining to him obtained by each such agency for a particular purpose from being used or made available for another purpose without his consent;~~

(3) permit an individual to gain access to certain Federal agency records pertaining to him, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or negligent action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS. For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the

~~United States or an alien lawfully admitted for permanent residence;~~

~~"(3) the term 'maintain' includes maintain, collect, use, or disseminate;~~

~~"(1) the term 'record' means any collection or grouping of data about an individual that is maintained by an agency and that contains his name, identifying number, symbol, or other identifying particular assigned to each such individual;~~

~~"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to each such individual; and~~

~~"(6) the term 'statistical research or reporting record' means a record in a system of records assembled or maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13, United States Code.~~

~~"(b) CONDITIONS OF DISCLOSURE. No agency shall disclose any record to any person, or to another agency, except pursuant to a written request by, or with the prior~~

written consent of, the individual to whom the record pertains, unless disclosure would be—

"(1) to those officers and employees of that agency who have a need for such record in the performance of their duties;

"(2) required pursuant to section 552 of this title or any other Federal statute;

"(3) for a routine use described in any rule promulgated pursuant to subsection (e)(4);

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey pursuant to the provisions of title 13, United States Code;

"(5) where the agency determines that the recipient of such record has provided advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and is to be transferred in a form that is not individually identifiable;

"(6) when transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

~~"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity if such activity is authorized by statute and if the head of such agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought; or~~

~~"(8) pursuant to a showing of compelling circumstances affecting the health, safety, or identification of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.~~

~~"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—~~

~~"(1) keep an accurate accounting of—~~

~~"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency, except for disclosures made pursuant to subsection (b) (1) through (6); and~~

~~"(B) the name and address of the person or agency to whom such disclosure is made;~~

"(2) retain the accounting made pursuant to paragraph (1) for at least five years after the disclosure for which such accounting is made;

"(3) except for disclosures made pursuant to subsection (b)(7), make the accounting available to the individual named therein at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of any record that has been disclosed to such person or agency within two years preceding the making of such correction of the individual's record, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section and for which there is no accounting of such disclosure.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to any record pertaining to him which is contained in any particular system of records maintained by the agency, permit him to gain access to such record and have a copy made of all or any portion thereof in a form comprehensible to him;

"(2) permit such individual to request amendment of a record pertaining to him and either—

"(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(B) promptly inform such individual of its refusal to amend such record in accordance with his request, the reason for such refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

"(3) permit any such individual who disagrees with the agency's refusal to amend his record to request review of such refusal by the official named in accordance with paragraph (2) (B); and if, after such review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the agency's refusal; and

"(4) in any disclosure relevant to such individual's disagreement occurring after the filing of the statement under paragraph (3), clearly note any portion of such record which is disputed and provide copies of such statement and, if the agency deems it appropriate, copies of a concise statement of the agency's reasons for

not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed.

"(e) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules in accordance with the requirements, including that of general notice, of section 553 of this title. Such rules shall—

"(1) include a notice of the existence and character of each system of records which the agency maintains, which notice shall consist of—

"(A) the name and location of each such system;

"(B) the categories of individuals on whom records are maintained in such system;

"(C) the categories of information maintained in such system; and

"(D) the title and business address of the agency official or employee who is responsible for such system;

"(2) establish procedures whereby an individual from whom information pertaining to him is being requested is apprised of the general purposes for which such information will be used;

"(3) describe the policies and practices of the

agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(4) describe for each system of records, each routine purpose for which the records contained in such system are used or intended to be used, including the categories of users of the records for each such purpose;

"(5) provide that any record which is used by the agency in making any determination about any individual is maintained with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness to the individual in such determination;

"(6) establish procedures whereby an individual can be notified in response to his request if any particular system of records contains a record pertaining to him;

"(7) define reasonable items, places, and requirements for identifying individuals who request records pertaining to themselves before the agency shall make such records available to such individuals;

"(8) establish procedures for the disclosure to an individual upon his request of records pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(9) establish procedures for reviewing requests from individuals concerning the amendment of records pertaining to such individuals, for making a determina-

~~tion on such requests, for appeals within the agency of initial adverse agency determinations, and for whatever additional means the head of the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and~~

~~"(10) establish fees to be charged, if any, to individuals for making copies of their records, excluding the cost of any search for such records and review of them.~~

~~"(f) (1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d) (1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to such individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such records and consequently makes such a determination which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, such individual may bring a civil action against such agency, and the district courts of the United States shall have jurisdiction in such matters as provided by paragraph (4) of this subsection.~~

~~"(2) (A) In any suit brought pursuant to the provisions~~

~~of subsection (f) (1), the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether such records or any portion thereof may be withheld under any of the exemptions set forth in subsection (i) or (j) of this section, and the burden is on the agency to sustain its action.~~

~~"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.~~

~~"(3) In any suit brought pursuant to the provisions of subsection (f) (1) in which the court determines—~~

~~"(A) that the agency's refusal or failure has been willful, the agency shall be liable to the individual in an amount equal to the sum of—~~

~~"(i) actual damages sustained by the individual as a result of such refusal or failure;~~

~~"(ii) punitive damages allowed by the court; and~~

~~"(iii) the costs of the action together with reasonable attorney's fees as determined by the court;~~

or

"(B) that the agency's refusal or failure has been negligent, the agency shall be liable to the individual in an amount equal to the sum of—

"(i) any actual damages sustained by the individual as a result of such refusal or failure; and

"(ii) the costs of the action together with reasonable attorney's fees as determined by the court.

"(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the agency's liability to that individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

"(g) RIGHTS OF LEGAL GUARDIANS.—For the purposes of subsections (b), (d), and (f) of this section, the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age

by a court of competent jurisdiction may act on behalf of such individual.

"(h) (1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information, the disclosure of which is prohibited by this section or by rules or regulations established pursuant thereto, and who knowing that disclosure of such specific material is so prohibited, willfully discloses such material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.

"(i) GENERAL EXEMPTIONS. Except for subsections (c) (1) and (c) (3), the provisions of this section shall not apply to any record or system of records which is—

"(1) maintained by any agency to the extent that the President determines by Executive order, on an annual basis, that providing access by an individual to his records would cause serious damage to the national defense or foreign policy;

"(2) maintained by the Central Intelligence Agency; or

"~~(3) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (a) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (b) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (c) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.~~

"~~(j) SPECIFIC EXEMPTIONS.—Subsections (b), (c) (3), (d), (e) (2), and (e) (6) through (10) shall not apply to any record or system of records which is—~~

"~~(1) subject to the provisions of section 552 (b) (1) of this title;~~

"~~(2) investigatory material compiled for law en-~~

~~forcement purposes, except to the extent that such material is within the scope of paragraph (i) (3) or is open to public inspection under the provisions of section 552 (b) (7) of this title;~~

~~"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18, United States Code;~~

~~"(4) investigatory material maintained for the purpose of determining initial or continuing eligibility or qualification for Federal employment, military service, Federal contracts, or access to classified information;~~

~~"(5) material used for appointment, employment, or promotion in the Federal service; or~~

~~"(6) required by statute to be maintained and used solely as statistical research or reporting records.~~

~~"(k) (1) ARCHIVAL RECORDS. Agency records which are accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44, United States Code, shall, for the purposes of this section, be considered to be maintained by the agency which deposited the records and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose such records, or any information therein, except to the agency which maintains the records or pursuant to rules established by that agency.~~

"~~(2) Agency records pertaining to identifiable individuals which were transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section.~~

"~~(3) Agency records pertaining to identifiable individuals which are transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsection (e)(1); (d)(2), (3), and (4); (e)(2), (5), and (9); (f)(1)(B) and (C); and (f)(3).~~

"~~(l) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section pursuant to the provisions of subsections (i) and (j) of this section during~~

the preceding calendar year, and the reasons for such exemptions, and such other information as indicates efforts to administer fully this section."

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings."

SEC. 5. (a) Title 44, United States Code, is amended by adding after section 3506 the following new section:

"§ 3506a. Information concerning political and religious beliefs and activities

"No Federal agency shall maintain any record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained."

(b) The chapter analysis of chapter 35 of title 44, United States Code, is amended by inserting:

"3506a. Information concerning political and religious beliefs and activities."

immediately below:

"3506. Determination of necessity for information; hearing."

SEC. 6. The amendments made by this Act shall become effective on the one hundred and eightieth day following the date of enactment of this Act, except that the amendments

~~made with respect to section 552a(c) of title 5, United State Code, shall become effective on the date of enactment of this Act.~~

That this Act may be cited as the "Privacy Act of 1974".

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Con-

gress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases

63-619 O - 76 - 19

where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful, arbitrary, or capricious action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any collection or grouping of information about an individual that is maintained by an agency and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual;

"(5) the term 'system of records' means a group of any records under the control of any agency from which

information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual; and

"(6) the term 'statistical research or reporting record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) for a routine use described in any rule promulgated under subsection (e)(2)(D) of this section;

"(3) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(4) to a recipient who has provided the agency with advance adequate written assurance that the record

will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(5) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(6) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(7) pursuant to a showing of compelling circumstances affecting the health or safety of an individual, if upon the disclosure notification is transmitted to the last known address of the individual; or

"(8) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsection (b)(1) of this section or disclosures to the public from records which by law or regulation are open to public inspection or copying, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(6) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency within two years preceding the making of the correction

of the record of the individual, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section or for which no accounting of the disclosure is required.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him to review the record and have a copy made of all or any portion thereof in a form comprehensible to him;

"(2) permit the individual to request amendment of a record pertaining to him and either—

"(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(B) promptly inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

"(3) permit any individual who disagrees with the refusal of the agency to amend his record to request re-

view of the refusal by the official named in accordance with paragraph (2)(B) of this subsection; and if, after the review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency; and

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and, upon request, provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) which Federal statute or regulation, if any, requires disclosure of the information;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) other purposes for which the information may be used, as published pursuant to paragraph (2)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

"(2) publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine purpose for which the records contained in the system are used or intended to be used, including the categories of users of the records for each such purpose;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an in-

dividual can be notified at his request if the system of records contains a record pertaining to him; and

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content;

"(3) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; and

"(4) maintain no record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained.

"(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means the head of the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d)(1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of records and consequently a determination is made which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

"(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (j) or (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(3) In any suit brought under the provisions of subsection (g)(1) (B) or (C) of this section in which the court determines that the agency acted in a manner which was willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—

"(A) actual damages sustained by the individual as a result of the refusal or failure; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be brought at any

time within two years after discovery by the individual of the misrepresentation.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from any

part of this section except subsections (b) and (e)(2)(A) through (F) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements

(including general notice) of section 553 of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(2) (G) and(H), and (f) of this section if the system of records is—

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, except to the extent that the material is within the scope of subsection (j)(2) of this section or is open to public inspection under the provisions of section 552(b)(7) of this title;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18; or

"(4) required by statute to be maintained and used solely as statistical research or reporting records.

"(l)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the

record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsections (c)(4); (d) (2), (3), and (4); (e) (1), (2)(H) and (3); (f)(4); (g)(1)(B) and (C), and (3).

"(m) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records

contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.".

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings.".

SEC. 5. The amendments made by this Act shall become effective on the one hundred and eightieth day following the date of enactment of this Act.

63-619 O - 76 - 20

93D CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
2d Session } { No. 93-1416

PRIVACY ACT OF 1974

OCTOBER 2, 1974.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

MR. MOORHEAD of Pennsylvania, from the Committee on Government Operations, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany H.R. 16373]

The Committee on Government Operations, to whom was referred the bill (H.R. 16373) to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment to the text of the bill strikes out all after the enacting clause and inserts a substitute text which appears in italic type in the reported bill.

DIVISIONS OF THE REPORT

Summary and purpose.
Background.
Committee action and vote.
Discussion:
- Definitions.
- Conditions of disclosure.
- Accounting of certain disclosures.
- Access to records.
- Agency requirements.
- Agency rules.
- Civil remedies.
- Rights of legal guardians.
- Criminal penalties.
- General exemptions.

Specific exemptions.
Archival records.
Annual report.
Technical changes.
Effective date.
Cost estimate.
Agency views.
Section-by-section analysis.
Changes in existing law made by the bill, as reported.
Appendix: Correspondence regarding cost estimate.
Additional views.

Summary and Purpose

H.R. 16373 prescribes legislative guidelines within the framework of the Freedom of Information Act (5 U.S.C. 552) to protect the privacy of individuals by regulating the Federal Government's collection, maintenance, use, or dissemination of personal, identifiable information.

In summary, the bill:

1. Permits an individual to have access to records containing personal information on him kept by Federal agencies for purposes of inspection, copying, supplementation and correction (with certain exceptions, including law enforcement and national security records).

2. Allows an individual to control the transfer of personal information about him from one Federal agency to another for non-routine purposes by requiring his prior written consent.

3. Makes known to the American public the existence and characteristics of all personal information systems kept by every Federal agency.

4. Prohibits the maintenance by Federal agencies of any records concerning the political and religious beliefs of individuals unless expressly authorized by law or an individual himself.

5. Limits availability of records containing personal information to agency employees who need access to them in the performance of their duties.

6. Requires agencies to keep an accurate accounting of transfers of personal records to other agencies and outsiders and make such an accounting available, with certain exceptions to the individual upon his request.

7. Requires agencies, through formal rulemaking, to list and describe routine transfers and establish procedures for access by individuals to records about themselves, amending records, handling medical information, and charging fees for copies of documents.

8. Makes it incumbent upon an agency to keep records with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in making determinations about him.

9. Provides a civil remedy by individuals who have been denied access to their records or whose records have been kept or used in contravention of the requirements of the act. The complainant

may recover actual damages and costs and attorney fees if the agency's infraction was willful, arbitrary, or capricious.

10. Makes unlawful possession of or disclosure of individually identifiable information by a government employee punishable by a fine not to exceed $5,000.

11. Provides that any person who requests or obtains such a record by false pretenses is subject to a fine of not to exceed $5,000.

12. Sets forth statutory provisions relating to archival records; requires annual report from President on agency uses of exemptions; and provides that the law would become effective 180 days following enactment.

Hearings and investigations by subcommittees of the House Government Operations Committee over the past decade have revealed major violations of the privacy of individual American citizens by the Federal Government in its growing collection and use of personal data furnished by citizens for specific governmental purposes. Accelerated data sharing of such personally identifiable information among increasing numbers of Federal agencies through sophisticated automated systems, coupled with the recent disclosures of serious abuses of governmental authority represented by the collection of personal dossiers, illegal wiretapping, surveillance of innocent citizens, misuse of income tax data, and similar types of abuses, have helped to create a growing distrust, or even fear of their Government in the minds of millions of Americans.

H.R. 16373 provides a series of basic safeguards for the individual to help remedy the misuse of personal information by the Federal Government and reassert the fundamental rights of personal privacy of all Americans that are derived from the Constitution of the United States. At the same time, it recognizes the legitimate need of the Federal Government to collect, store, use, and share among various agencies certain types of personal data. This information includes income tax returns, Social Security records, veterans' medical and service records, civil service records, census data, economic statistics, governmental payroll records, law enforcement records, and other similar types of personally identifiable information about many millions of individuals.

H.R. 16373 provides that each agency covered by it administer its provisions independently, subject to the guidelines created by law and agency regulations implementing each operative part. Regulations are subject to standard rulemaking requirements of the Administrative Procedure Act (title 5, section 553, United States Code).

Like the Freedom of Information Act, H.R. 16373 also recognizes that certain areas of Federal records are of such a highly sensitive nature that they must be exempted from its provisions. The measure provides a general exemption from most of the bill's operative provisions to systems of records maintained by the Central Intelligence Agency and those used for criminal justice purposes such as computerized systems of the National Crime Information Center (NCIC), maintained by the Federal Bureau of Investigation, and other Federal criminal history file systems. Other committees of the Congress

have been studying this aspect of the privacy issue and currently have pending separate bills to provide safeguards in the criminal justice information area.

H.R. 16373 also permits the head of an agency to exempt certain other types of record systems, subject to his written determination of the reasons to be published in the *Federal Register*. These include systems of records that—(1) are subject to withholding under section 552(b)(1) of the Freedom of Information Act, relating to classified national defense or foreign policy information; (2) consist of certain types of investigatory material compiled for law enforcement purposes; (3) relate to protective services rendered the President of the United States and others, such as those records maintained by the Secret Service; and (4) are required by other statutes to be maintained and used solely as statistical reporting or research records.

Under the provisions of this legislation, however, Federal agencies (even those to which these exemptions apply) would be required to publish annually in the Federal Register certain identifying characteristics about virtually all systems of records under their control from which personally identifiable information could be retrieved. The objective of the bill is that there be no "secret" government system of records containing personal information about individuals.

Also like the Freedom of Information Act, H.R. 16373 provides for the exercise of civil remedies by individuals against the Federal Government through the Federal courts to enforce their rights, with the burden of proof resting on the government. Provision is made for the collection of actual damages by the individual against the government if the infraction was willful, arbitrary, or capricious, and the court may award the complainant court costs and attorney fees in its discretion. Penalties are also provided for the unauthorized knowing and willful disclosure of individually identifiable material by a government officer or employee by a fine of not more than $5,000. Criminal penalties and fines would be imposed on persons requesting or obtaining any such individually identifiable record under false pretenses.

H. R. 16373 attempts to strike that delicate balance between two fundamental and conflicting needs—on the one hand, that of the individual American for a maximum degree of privacy over personal information he furnishes his government, and on the other, that of the government for information about the individual which it finds necessary to carry out its legitimate functions.

Background

Public and Congressional concern over an increasing trend within our government to snoop into virtually every segment of our society is not new.

George Orwell's famous book *1984*, published a generation ago, focused public attention on the fictional fishbowl existence of human life in the "Big Brother" era and the potential threats to any free system posed by some political-technical-social innovations.

During the "cold war" period of the late 1940s and 1950s, widespread abuses engulfed various governmental and private efforts to ferret out alleged "subversives." Intellectual dissent was driven some-

what into hiding. Terms such as "security risk," "loyalty oaths," "pinko," and "guilt by association" came into common usage during what later became known as the "McCarthy era" of the early half of the 1950s. Many Americans were required to defend publicly their loyalty during "star-chamber" proceedings, often despite years of service to our Nation during war and peacetime. Indiscriminate use of dubious "informers," wiretapping, surveillance, neighborhood snooping, and other flagrant invasions of personal privacy were seen more and more.

In the 1960s the former Special Subcommittee on Government Information of this committee launched extensive investigations into the practice of telephone monitoring and the use of so-called "lie detectors" by Federal agencies. Hearings, studies and reports based on these investigations revealed numerous examples of privacy invasion affecting Federal employees and the public in their dealings with Federal agencies.[1]

Late in 1964, the chairman of the Government Operations Committee created a Special Subcommittee on Invasion of Privacy, which began inquiries into Federal agency investigative activities, the proposed establishment of a National Data Bank by the government, computerized personal recordkeeping, and related privacy matters. Hearings were held during 1965 and 1966 into such issues and a report, concentrating on the National Data Bank concept was issued by the Committee in 1968.[2] The Special Subcommittee also held hearings in 1968 on the privacy abuses inherent in the operation of private commercial credit reporting organizations.[3] The Foreign Operations and Government Information Subcommittee of this Committee in 1970 updated the earlier studies and reports on Federal agency telephone monitoring practices.[4]

Increasing concern over invasion of privacy during the 1960s resulted in Congressional efforts to deal with aspects of the problem on a piecemeal basis. The enactment of the Fair Credit Reporting Act of 1970 was directed at many of the privacy abuses uncovered by the Special Subcommittee on Invasion of Privacy two years earlier.[5] The investigation of military surveillance over American political dissidents by the Senate Subcommittee on Constitutional Rights headed by Senator Ervin revealed yet another dimension of abuses during the late 1960's involving intelligence gathering activities that violated

[1] H. Rept. 1215, 87th Cong., 1st sess. "Availability of Information from Federal Departments and Agencies (Telephone Monitoring)," Sept. 19, 1961. H. Rept. 1898, 87th Cong., 2d sess. "Availability of Information from Federal Departments and Agencies (Telephone Monitoring—Second Review)," June 22, 1962. "Use of Polygraphs by the Federal Government (Preliminary Study)." Committee Print, 88th Cong., 2d sess., Apr., 1964. Hearings, Foreign Operations and Government Information Subcommittee, 88th Cong., 2d sess., "Use of Polygraphs as 'Lie Detectors' by the Federal Government." Parts 1–4, Apr. and May, 1964. Parts 5–6, May and Aug., 1965. H. Rept. 198, 89th Cong., 1st sess. "Use of Polygraphs as 'Lie Detectors' by the Federal Government," part 1, Mar. 22, 1965; H. Rept. 2081, 89th Cong., 2d sess., "Use of Polygraphs as 'Lie Detectors' by the Federal Government," part 2, Sept. 26, 1966.

[2] Hearings, Special Subcommittee on Invasion of Privacy, "Special Inquiry on Invasion of Privacy," part 1, June and September 1965; part 2, May 1966. "The Computer and Invasion of Privacy," July 1966. H. Rept. 1842, 90th Cong., 2d sess., "Privacy and the National Data Bank Concept," Aug. 2, 1968.

[3] Hearings, Special Subcommittee on Invasion of Privacy, 90th Cong., 2d sess., "Commercial Credit Bureaus," March 1968, hearings, "Retail Credit Co. of Atlanta, Georgia," May 1968.

[4] "Availability of Information from Federal Departments and Agencies (Telephone Monitoring—Third Review)" Committee Print, 91st Cong., 2d sess., December 1970.

[5] Public Law 91–508; 15 U.S.C. 1601 et seq.

basic privacy rights.[6] Such actions were prompted by the rash of civil disturbances and racial and political unrest on college campuses.

A survey and hearings by the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committee in 1965, 1966, and 1967 had already explored such areas as electronic eavesdropping, wiretapping, the Federal Government's collection of personal data, lie detectors, surveillance activities, and other privacy issues. In a November, 1967, publication entitled "Government Dossiers (Survey of Information Contained in Government Files)" that subcommittee reported the results of a survey of Federal agencies as to the types of information collected and maintained by government on individuals. The results of this survey were important in identifying data systems that could be subject to regulation and in the subsequent drafting of legislation to curb governmental privacy abuses.[7]

Also during this same period, legislation was first considered to protect the Constitutional rights to privacy of Federal employees. The Ervin bill has been passed by the Senate during each of the past several Congresses, but it has never been acted upon in the House.[8]

Much of the Congressional investigative and legislative activity in recent years to deal with the rising tide of privacy-related abuses in the public and private sectors has been spear-headed by the Senate Constitutional Rights Subcommittee. However, other types of legislation to assure individual safeguards against the misuse of personal data held by Federal agencies was being introduced in the House by Representative Koch and many other Members. Hearings were held in June 1972 on such legislation (H.R. 9527) by the Foreign Operations and Government Information Subcommittee of this committee, but no further action was taken before adjournment of the 92nd Congress. The bill was the forerunner of revised and separate versions introduced by many other Members of the House in 1973 and 1974, on which H.R. 16373 is based.[9]

A study by the National Academy of Sciences Project on Computer Databanks was also published in 1972. Entitled "Databanks in a Free Society," this study outlined what the use of computers is actually doing to record-keeping processes in the United States, and what the growth of large-scale databanks—both manual and automated—implies for the individuals' constitutional right to privacy and due process.[10]

---

[6] For a detailed summary of Army surveillance and intelligence activities over civilians, see article by Christopher H. Pyle, "CONUS Revisited: The Army Covers Up" in a collection of materials compiled and published as a Committee Print by the Congressional Research Service, Library of Congress relating to the 1971–1972 Intercollegiate debate topic, "Resolved: That More Stringent Control Should be Imposed Upon Government Agencies Gathering Information About United States Citizens." H. Doc. 92–167, pp. 207–218.

[7] Ibid., "Survey of Information Contained in Government Files," pp. 33–39.

[8] Ibid. The Congressional Research Service compilation included a legislative history of Congressional action involving various Ervin bills; see pp. 101–115. "S. 782—A Bill to Protect the Constitutional Right to Privacy of Federal Employees," by Robert M. Foley and Harold P. Coxson; originally copyrighted and published in the American University Law Review, vol. 19, June–August 1970, pp. 532–549.

[9] Hearings, Foreign Operations and Government Information Subcommittee, "Records Maintained by Government Agencies," on H.R. 9527 and related bills; 92d Cong., 2d sess., June 1973; "Access to Records," on H.R. 12206 and related bills; 93d Cong., 2d sess., February, April, and May 1974.

[10] Alan F. Westin and Michael A. Baker, *Databank in a Free Society*, report of the Project on Computer Databanks, Computer Science and Engineering Board, National Academy of Sciences. New York: Quadrangle Books, 1972. For a summary of the report, see Hearings, Foreign Operations and Government Information Subcommittee, "Federal Information Systems and Plans—Implications and Issues," part 3. 93d Cong., 2d sess., January and February 1974. Pp. 1190–1196.

During this same period, Elliott Richardson, then Secretary of Health, Education and Welfare, named an Advisory Committee on Automated Personal Data Systems to make an intensive study of the impact of computer data banks on individual privacy. Its detailed report, "Records, Computers, and the Rights of Citizens," was published in 1973 and recommended the enactment of Federal legislation guaranteeing to all Americans a "code of fair information practices." [11] H.R. 16373 embodies the major principles of these recommendations as they apply to an individual's access to records in the Federal Government.

Late in 1972, meanwhile, the Foreign Operations and Government Information Subcommittee of this committee began an investigation of a comprehensive report the President's Domestic Council proposing a nationwide system of computer and communications technology to create "wired cities" and a "wired Nation." The report, entitled "Communications for Social Needs; Technological Opportunities," was prepared in 1971. Although the report was formally rejected, according to a White House spokesman, the "Big Brother" implications were another ominous indication of the possible threats to individual privacy in America. This investigation led to broad investigative hearings by the Subcommittee into advanced information technology and the use of information systems by the Federal Government. These hearings began in April 1973, and concluded early in 1974. They were a useful adjunct to the legislative hearings on H.R. 16373 and its legislative forerunners, which they closely paralleled.[12]

Another related investigation affecting individual privacy was also conducted by the Subcommittee during this same period. It involved the issuance of a Presidential Executive order in January 1973 to permit the Agriculture Department to inspect some 3 million income tax returns of persons having farming operations for the purpose of compiling special mailing lists to make statistical surveys. Hearings were held in May and August 1973. The order aroused widespread public concern and opposition and was strongly criticized in the subsequent unanimous report issued by the Committee in October 1973.[13] In the interim, the Internal Revenue Service had postponed implementation of the order and it was finally rescinded in the spring of 1974.[14]

The growing concern of Americans of all walks of life to the threat of a "Big Brother" society well in advance of 1984 has been reflected in the Congress. During the last two years, more than 100 Members of Congress of both parties and of all shades of political ideology have

---

[11] "Records, Computers, and the Rights of Citizens," a report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare, July 1973. DHEW Publication No. (OS)73-94. See "Summary and Recommendations," p. xxiii.

[12] Hearings, Foreign Operations and Government Information Subcommittee, 93d Cong., 1st and 2d sess., "Federal Information Systems and Plans—Federal Use and Development of Advanced Information Technology" (Part 1, April 1973); (part 2, June and July 1973); "Federal Information Systems and Plans—Implications and Issues" (part 3, January and February 1974).

[13] Hearings, Foreign Operations and Government Information Subcommittee, 93d Cong., 1st sess., "Executive Orders 11697 and 11709 Permitting Inspection by the Department of Agriculture of Farmers' Income Tax Returns," May and August 1973; H. Rept. 93-598, 93d Cong., 1st sess., "Information from Farmers' Income Tax Returns and Invasion of Privacy," Oct. 18, 1973.

[14] ——— F.R. ——— 1974; additional attention on invasion of privacy aspects of the Executive orders was focused by the Domestic Council Committee on the Right of Privacy, headed by then Vice President Ford.

introduced or co-sponsored legislation to impose effective safeguards on both government and business in their collection and use of personal data.

In June 1974, the Foreign Operations and Government Information Subcommittee of this committee held extensive hearings on the Federal Government's telephone monitoring practices and the use of "lie detectors" and other similar newer devices, thus updating the earlier Subcommittee studies in these areas during the 1960s.[15] These hearings also paralleled consideration of H.R. 16373 during its markup stages.

Former President Nixon's State of the Union Message to Congress on January 30, 1974, also took note of the need to protect individual privacy. He said:[16]

> One of the basic rights we cherish most in America is the right of privacy. With the advance of technology, that right has been increasingly threatened. The problem is not simply one of setting effective curbs on invasions of privacy, but even more fundamentally one of limiting the uses to which essentially private information is put, and of recognizing the basic proprietary rights each individual has in information concerning himself.
>
> Privacy, of course, is not absolute; it may conflict, for example, with the need to pursue justice. But where conflicts occur, an intelligent balance must be struck.
>
> One part of the current problem is that as technology has increased the ability of government and private organizations to gather and disseminate information about individuals, the safeguards needed to protect the privacy of individuals and communications have not kept pace. Another part of the problem is that clear definitions and standards concerning the right of privacy have not been developed and agreed upon.

To carry forward these efforts he established on February 23, 1974, a cabinet-level "Committee on the Right of Privacy" within the White House's Domestic Council headed by then Vice President Gerald R. Ford. At its July 10, 1974, meeting, that committee urged the enactment of privacy legislation embodying the principles contained in H.R. 16373, along with a number of other important "privacy initiative" measures.[17]

Additional impetus in Congress to enact privacy safeguards into law has resulted from recent revelations connected with Watergate-related investigations, indictments, trials, and convictions. They included such activities as the break-in at the Democratic National Committee's headquarters in June 1972, the slowly emerging series of revelations of "White House enemies' lists," the break-in of the office of Daniel Ellsberg's psychiatrist, the misuse of CIA-produced "personality profiles" on Ellsberg, the wiretapping of the phones of government employees and news reporters, and surreptitious taping of

---

[15] Hearings, Foreign Operations and Government Information Subcommittee, 93d Cong., 2d sess., "The Use of Polygraphs and Similar Devices by Federal Agencies," June 1974; "Telephone Monitoring Practices by Federal Agencies," June 1974.

[16] *Congressional Record*, Jan. 30, 1974 (daily edition), p. H372.

[17] Domestic Council Committee on the Right of Privacy, "Fact Sheet on Meeting of Committee, issued July 10, 1974, see "Proposed Initiative No. 9," p. 4.

personal conversations within the Oval Office of the White House as well as political surveillance, spying, and "mail covers."

Other important support for prompt action to preserve the individual's right to privacy from further erosion has come from individual computer companies and trade associations representing every segment of the American computer industry. These experts presented testimony stressing the importance of privacy and the safeguarding of the integrity of stored data on individuals during the Foreign Operations and Government Information Subcommittee's hearings on information technology early in 1974.[18] A recent nationwide IBM institutional advertisement, entitled "Four Principles of Privacy," endorsed these basic purposes as "sound public policy" cornerstones:[19]

> 1. Individuals should have access to information about themselves in record-keeping systems. And there should be some procedure for individuals to find out how this information is being used.
>
> 2. There should be some way for an individual to correct or amend an inaccurate record.
>
> 3. An individual should be able to prevent information from being improperly disclosed or used for other than authorized purposes without his or her consent, unless required by law.
>
> 4. The custodian of data files containing sensitive information should take reasonable precautions to be sure that the data are reliable and not misused.

As they apply to record-keeping activities of the Federal Government, these are also among the basic principles of privacy protection that are contained in H.R. 16373.

The broad principles involved in what is conveniently called "the individual right of privacy" are deeply rooted in our history and derived from the Bill of Rights of the United States Constitution. The fourth amendment to the Constitution was written as the result of the American colonial experience with warrants and writs issued under King George III of England which often gave his officers an excuse to search anyone, anywhere, any time. Even then an English Chief Justice—Pratt, later Lord Camden —in commenting upon such a search conducted against John Wilkes, said:[20]

> To enter a man's house by virtue of a nameless warrant, in order to procure evidences, is worse than the Spanish Inquisition—a law under which no Englishman would wish to live an hour.

In their famous 1890 *Harrard Law Review* article "The Right to Privacy," Samuel Warren and Louis D. Brandeis concluded:[21]

> It would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required . . . The

---

[18] See Hearings, "Federal Information Systems and Plans," op. cit., part 3, testimony from technical experts in information system industry.

[19] "IBM Reports—Four Principles of Privacy," full page advertisement, *Newsweek*, July 8, 1974, p. 48.

[20] Hearings, Special Subcommittee on Invasion of Privacy, "Special Inquiry on Invasion of Privacy," op. cit., p. 4.

[21] 4 *Harvard Law Review* 193 (1890).

> common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?

Almost 40 years later, Justice Brandeis, in his famous dissent in the case of *Olmstead* v. *United States*, set forth the basic Constitutional principles of individual privacy: [22]

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect * * *. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable instrusion by the Government upon the privacy of the individual, whatever the means employed must be deemed a violation of the fourth amendment.

He went on to say further in his dissent, even more relevant in these days of wholesale abuses of governmental power in our modern computerized society:

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasions to their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding.

While there can be no right of *absolute* privacy in our complex civilization, there is an urgent need today to assert the fundamental right of privacy for all Americans to the maximum extent consistent with the overall welfare of our Nation. The Federal Government can and must take the lead to achieve this important objective. Congress has the opportunity to mandate such action by acting promptly to enact H.R. 16373 into law.

On August 12, 1974, in his first address to the Congress as Chief Executive, President Ford pledged his personal and official dedication to the individual right of privacy. He declared, "There will be hot pursuit of tough laws to prevent illegal invasion of privacy in both government and private activities." The Committee offers H.R. 16373 as the first step in that pursuit.

Committee Action and Vote

As noted above, the issues involved in the safeguarding of individual privacy have been the subject of numerous investigatory hearings by the Foreign Operations and Government Information Subcommittee of this committee during the past several years.

---

[22] *Olmstead* v. *United States*, 277 U.S. 438 (1928); quoted in Hearings, Special Subcommittee on Invasion of Privacy, "Special Inquiry on Invasion of Privacy," op, cit., pp. 3–4.

Public hearings on specific legislative proposals related to H.R. 16373 were held by the Subcommittee in June 1972, and in February, April, and May 1974, on a number of revised privacy measures—H.R. 12206, H.R. 12207, H.R. 13303, H.R. 13304, H.R. 13872, H.R. 14493, etc.

Subcommittee markup sessions were held in May, June, and July to draft effective and workable language to reach a balance between the individual's rights to privacy and the government's need for personal information. During this period, much of the technical detail of H.R. 16373 was worked out in informal meetings among the Subcommittee's staff, the assistant minority counsel for the Committee, officials of the Office of Management and Budget, and representatives of the Vice President's Committee on the Right of Privacy.

After agreement in principle was reached by the Subcommittee on most of the specific language, a clean bill—H.R. 16373—was introduced by Subcommittee Chairman Moorhead on August 12, 1974, cosponsored by 13 Members, including several leading sponsors of privacy protection legislation in the House. The bill was subsequently reported favorably by the Subcommittee on September 12, 1974, without a dissenting vote.

The Government Operations Committee considered H.R. 16373 on September 19, 1974, and favorably reported it to the House on September 24, 1974, by a roll call vote of 39 to 0.

Discussion

Because of the complex interrelationships of the major provisions of this legislation, each of its subsections is explained in detail in this part of the report.

DEFINITIONS

Section 3 of H.R. 16373 sets forth the new privacy protection section 552a of title 5, United States Code, and in section (a) provides six definitions of terms used in the new section:

Section (a)(1) defines the term "agency."

Section (a)(2) defines the term "individual" as affected by this measure as a "citizen of the United States or an alien lawfully admitted for permanent residence" in the United States; thus, it would not affect any other foreign nationals.

Section (a)(3) defines the term "maintain" with respect to agency records to include the other terms "collect, use, or disseminate;".

Section (a)(4) defines the term "record" as "any collection or grouping of information about an individual that is maintained by an agency and that contains his name or identifying number, symbol, or other identifying particular assigned to such individual." This encompasses records contained in either manual files or automated or computerized forms.

Section (a)(5) defines the term "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to each such individual;".

Section (a)(6) defines the term "statistical reporting or research record" as "a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13, United States Code." This latter provision permits the Census Bureau to furnish transcripts of census records for genealogical and other proper purposes and to make special statistical surveys from census data for a fee upon request.

CONDITIONS OF DISCLOSURE

Section 552a (b) provides that no Federal agency shall disclose any record containing personal information about an individual without his approval to any person not employed by that agency or to another agency except under certain special conditions.

The consent requirement may well be one of the most important, if not the most important, provisions of the bill. No such transfer could be made unless it was pursuant to a written request by the individual or by his prior written consent. This requirement would apply to all so-called "non-routine" transfers of information. It is not the Committee's intent to impede the orderly conduct of government or delay services performed in the interests of the individual. Under the conditional disclosure provisions of the bill, "routine" transfers will be permitted without the necessity of prior written consent. A "non-routine" transfer is generally one in which the personal information on an individual is used for a purpose other than originally intended.

Agencies will be required to publish annually in the Federal Register a description of each "routine" purpose for which personal information records are used or intended to be used. The Committee intends to exercise a vigorous oversight check on agencies to make certain as much as possible that no "non-routine" transfers of records of the type requiring prior written consent are either hidden or blanketed in under the "routine" category to nullify the basic protections of the law to individuals.

Another exception to the consent requirement is where a personal information record is transferred to another agency, including state and local instrumentalities, for a law enforcement activity if such activity is authorized by law and if the head of the agency seeking the information has made a written request specifying the particular portion desired and the criminal or civil law enforcement activity for which the record is sought.

A record cannot be transferred to another agency for statistical reporting or research purposes unless it is in a form that is not individually identifiable. This, for example, would prohibit such things as the transfer of personal financial information on income tax returns of farmers to the Department of Agriculture without the prior written consent of farmers.

An exception to this requirement would be made for the transfer of records to the Bureau of the Census for purposes of planning or carrying out a census, survey, or related activity. Laws relating to the Bureau of the Census are very strict, limiting access to such records only to Census employees and prohibiting their removal from the

premises and control of the Bureau. Even the Federal Bureau of Investigation is not permitted to examine individual Census records. The Committee believes the privacy rights of individuals already are adequately protected in the case of Census records and the Bureau of the Census is not involved in making individual program determinations comparable to other agencies.

The Committee is of the view that special consideration must be given to valid emergency situations, such as an airline crash or epidemic, where consent cannot be obtained because of time and distance and instant action is required, perhaps as a matter of life or death. The bill provides that in these situations record transfers can be made without the usual prior written consent if, on such disclosure, notification is transmitted to the individual's last known address. This provision is necessary so that government doctors and other Federal employees are not in the position of being technically in violation of the law.

The legislation also waives the consent provision when personal information is transferred to the National Archives as a record which has sufficient historical or other value to warrant its continued preservation by the government. In any case, the archival record protections contained in (1)(1) would apply to such records.

The final exception in the disclosure section relates to personal information needed by the Congress and its committees and subcommittees. Occasionally, it is necessary to inquire into such subjects for legislative and investigative reasons.

This legislation would have an effect on subsection (b)(6) of the Freedom of Information Act (5 U.S.C. section 552), which states that the provisions regarding disclosure of information to the public shall not apply to material "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." H.R. 16373 would make all individually-identifiable information in Government files exempt from public disclosure. Such information could be made available to the public only pursuant to rules published by agencies in the Federal Register permitting the transfer of particular data to persons other than the individuals to whom they pertain.

The Committee does not desire that agencies cease making individually-identifiable records open to the public, including the press, for inspection and copying. On the contrary, it believes that the public interest requires the disclosure of some personal information. Examples of such information are certain data about government licensees, and the names, titles, salaries, and duty stations of most Federal employees. The Committee merely intends that agencies consider the disclosure of this type of information on a category-by-category basis and allow by published rule only those disclosures which would not violate the spirit of the Freedom of Information Act by constituting "clearly unwarranted invasions of personal privacy."

Last, the Committee is cognizant of the fact that the Federal Reports Act (chapter 35 of title 44, United States Code) also restricts conditions of disclosure of personal information by government agencies. The purpose, scope, and administration of that act are different from similar aspects of H.R. 16373. Some records would be subject to the provisions of both the Federal Reports Act and this legislation,

however. The Committee intends that restrictions on the transfer of individually-identifiable data be as strong as they can be without impairing the ability of government agencies to perform their duties. It believes that the restrictions contained in this bill are stronger than the ones contained in section 3508(b) of title 44, U.S.C., and that they should consequently be followed with respect to the disclosure of personal information. Insofar as the restrictions of 44 U.S.C. section 3508 (b) may be stronger, however, the Committee intends that they should be followed.

ACCOUNTING OF CERTAIN DISCLOSURES

H.R. 16373 also provides in section 552a(c) that each agency shall keep an accurate accounting of the date, nature and purpose of each disclosure of a record to any person or to another agency, including the name and address of the person or agency to whom such disclosure is made. Exceptions to this would be when the record is used by employees of the same agency who need it in the performance of their duties and when disclosures are made to the public from records which by law or regulation are open to public inspection or copying.

The Committee has used the term "accounting," rather than "record," to indicate that an agency need not make a notation on a single document of every disclosure of a particular record. The agency may use any system it desires for keeping notations of disclosures, provided that it can construct from its system a document listing of all disclosures.

The agency must retain the accounting for at least five years and make it available to the individual concerned at his request, except for the part dealing with transfers for civil and criminal law enforcement purposes.

Under the provisions of section 552a(d), which are described below, an agency may correct an individual's record or note that a portion of the record is in dispute. Section (c) requires the agency to inform any person or other agency to whom it disclosed a record within two years preceding the making of the correction or notation of dispute about this amendment to the record.

Corrections or notations of dispute made to records disclosed prior to the effective date of the legislation or for which no accounting of a disclosure is required would be exempt from this requirement.

ACCESS TO RECORDS

Section 552a(d) grants each individual access to records pertaining to him which are maintained by government agencies and permits him to request amendment of his records. Each agency must under this provision make any correction of the documents which the individual requests or inform that person why it refuses to make the change and allow him to appeal the refusal within the agency.

Whenever an agency determines on appeal not to alter a record, it must permit the individual to file a concise statement of his reasons for disagreement. Additionally, it must make copies of that statement available to persons or agencies to whom it later transfers the disputed portion of the record.

The Committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them. The constant vigilance of individual citizens backed by legal redress is the best means, in the Committee's opinion, of making certain that government treats people fairly.

AGENCY REQUIREMENTS

Section 552a(e) is intended to ensure that all individuals may know the administrative structure of all systems of records; the uses to which such records will be put; and the procedures by which access, if mandated, may be had and inaccurate records contested. The section also requires that any record used to make a determination about an individual be maintained in an accurate, timely, and relevant fashion. By the term "determination" the Committee means any decision affecting the individual which is in whole or in part based on information contained in the record and which is made by any person or any agency.

Section (e)(1) requirements relate only to those records which are compiled from information received directly from the concerned individual. The purpose of these requirements is to ensure that individuals supplying information for a record system are fully aware of what the record will be used for and whether or not a response to the request is mandatory or voluntary.

Under section (e)(1)(D) the individual must be informed of the consequences of not providing any or all of the requested information. If the requested information is required to be provided by statute, the notification to the individual should indicate the statutory provision and its reach. If failure to provide the information could subject the individual to loss of a government benefit, the extent of such loss should be indicated. If there is no adverse effect on the individual for failure to comply with any or all of the request, that information should also be noted.

Section (e)(2) encompasses the public notice required to be made by each agency. The intent of this section is to ensure that the essential characteristics of all information systems covered by this Act are known to the public. The existence and character of each system, whether or not exempt from other requirements of this Act, must be published in the Federal Register as required by this section.

Under section (e)(2)(A) the name and location of each system must be published. If a system is located in more than one place, each location must be listed. Under section (e)(2)(B) the categories of individuals whose records are maintained in the system must be listed. The purpose of this requirement is to enable an individual to determine if information on him might be in such system. The description of the categories should therefore be clearly stated in non-technical terms understandable to individuals unfamiliar with data collection techniques.

Under section (e)(2)(C) the categories of records maintained should be listed in a manner similar to that of (e)(2)(B) so as adequately to inform individuals unfamiliar with data collection as to the kinds of records held in the system. The listing of "routine purposes" under (e)(2)(D) should include all uses to which the records will be put in the normal course of business. Transfer of a record for any use which is not published under this subsection will require a request by or prior written consent of the individual to whom the record pertains as provided under 552a(b).

Section (e)(2) (E) and (F) requires the agencies adequately to inform the public as to the policies governing the physical custody and protection of the record systems and to advise the public of the agency official who is responsible for the maintenance of the system.

The provisions of section (e)(2) (G) and (H) may be satisfied by publication of the applicable rules made under 552a(f).

In reference to the requirement in (e)(3) relating to "timeliness," the Committee intends this word to mean that a record was timely at the point when the determination by the agency about the individual was actually made.

Section (e)(4) prohibits the maintenance of any record under this Act which concerns the political or religious beliefs or activities of any individual as defined by this Act unless the individual authorizes the maintenance of such record or unless the maintenance of such record is expressly authorized by statute.

AGENCY RULES

Under section 552a(f) each agency must establish rules by which individuals may be apprised of information about them in record systems and by which such individuals may challenge inaccuracies in those records.

The rules required under (f) (1) through (5) must be promulgated in accordance with the provisions of 5 U.S.C. section 553.

Under section (f)(1) the agency is required to establish procedures whereby upon the request of an individual, the agency must notify him if the system which he names does or does not contain a record pertaining to him.

Under section (f)(2) each agency must promulgate rules by which an individual seeking access to his records can sufficiently identify himself as the individual named in the record. Such identification should if possible be made in person by the individual seeking access to his record. However, agencies should make efforts to ensure that individuals who are unable to appear at a designated location can satisfy identification requirements by other means.

Under (f)(3) each agency must establish procedures for disclosing pertinent records or information to individuals upon request. If a record contains information about more than one individual or contains other data not pertaining to the individual requesting the record, only the information pertaining to the requesting individual must be disclosed.

If, in the judgment of the agency, the transmission of medical information directly to a requesting individual could have an adverse effect upon such individual, the rules which the agency promulgates

63-619 O - 76 - 21

should provide means whereby an individual who would be adversely affected by receipt of such data may be apprised of it in a manner which would not cause such adverse effects. An example of a rule serving such purpose would be transmission to a doctor named by the requesting individual.

Under section (f)(4) each agency must establish rules by which an individual seeking to amend his record may have the request reviewed and if denied an initial review may appeal such denial.

This section additionally authorizes agency heads to promulgate such other rules as will enable individuals to enforce fully their rights under this Act.

Section (f)(5) authorizes the establishment of copying fees at the discretion of the agency. However, an agency may not charge the individual for time spent in searching for requested records or for time spent in reviewing records to determine if they fall within the disclosure requirements of the Act.

Finally, section (f) requires the publication of an annual compilation of all regulations promulgated by all agencies pursuant to this section.

The Office of the Federal Register is responsible for publication of this compilation and is directed to publish it in a form readily available to the public at low cost.

CIVIL REMEDIES

The section authorizing civil actions by individuals is designed to assure that any individual who has been refused lawful access to his record or information about him in a record, or has otherwise been injured by an agency action which was based upon an improperly constituted record, will have a remedy in the Federal District courts.

Actions may be brought if the agency refuses lawful access upon request of an individual. An action also lies if the agency makes an adverse determination based upon a record which is inaccurate, untimely, or incomplete. However, in order to sustain such action, the individual must demonstrate the causal relationship between the adverse determination and the incompleteness, inaccuracy, irrelevance or untimeliness of the record. Additionally, an action will lie for the failure of the agency to comply with any other section of this law when such non-compliance has an adverse effect upon the aggrieved individual.

The court may enjoin an agency from withholding records which do not fall within the exemptions set forth in sections 552a(j) or (k). The court is required to determine such matters *de novo* and the burden of proof is upon the agency to sustain the exemption.

Reasonable attorney fees and costs may be assessed against the government in any case where the plaintiff substantially prevails. It is intended that such award of fees not be automatic, but rather, that the courts consider the criteria as delineated in the existing body of law governing the award of fees. However, when an action is brought under section (g)(1)(B) or (C) and when the agency has been adjudged to have acted in a manner which was willful, arbitrary, or

capricious, the government shall be liable for reasonable attorney fees and costs.

In addition to the award of fees and costs, the United States is liable for actual damages resulting from the willful, arbitrary, or capricious action of an agency in a suit brought under section (g)(1)(B) or (C).

Venue lies in the district where the complainant resides or has his place of business, where the agency records are situated, or in the District of Columbia. The statute of limitations is two years from the date upon which the cause of action arises, except for cases in which the agency has materially or willfully misrepresented any information required to be disclosed and when such misrepresentation is material to the liability of the agency. In such cases the statute of limitations is two years from the date of discovery by the indicidual of the misrepresentation.

RIGHTS OF LEGAL GUARDIANS

Section (h) provides that the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction may act on behalf of such individual with respect to his rights under this law.

CRIMINAL PENALTIES

Any officer or employee of the United States who has access to or possession of a record the disclosure of which is prohibited by the Act or by the rules made pursuant to this act and who knowingly discloses such information to a person or agency not entitled to receive such information is liable for a fine of not more than $5,000.

Any person who knowingly and willfully obtains a record concerning an individual from any agency under false pretenses is liable for a fine of not more than $5,000.

GENERAL EXEMPTIONS

Section 552a(j) would permit the head of any agency to exempt certain systems of records within his agency from virtually all the requirements of the legislation. Only records maintained by the Central Intelligence Agency and criminal justice records could be so exempted. Even they would be subject to the requirements relating to conditions of disclosure (section 552a(b)) and publication of notice of the existence and character of each system of records (section 552a (e)(2)(A) through (F)).

The Committee believes that such a broad examination is permissible for these two types of records because they contain particularly sensitive information. C.I.A. files may include the most delicate information regarding national security. Criminal justice records are so different in use from other kinds of records that their disclosure should be governed by separate legislation.

The Committee has made certain, however, that a notice of the existence and character of these systems of records must be published at least annually in the *Federal Register*. We believe that the government should maintain no secret system of records about its own citizens. We have also made sure that systems may be exempted from certain re-

quirements of the bill only after the head of an agency promulgates rules which are open to public comment before they become effective. By this means, people will be afforded an opportunity to make their views on proposed exemptions known to the appropriate agencies, and agencies will be able to modify their decisions taking those views into account.

The Committee also wishes to stress that this section is not intended to require the C.I.A. and criminal justice agencies to withhold all their personal records from the individuals to whom they pertain. We urge those agencies to keep open whatever files are presently open and to make available in the future whatever files can be made available without clearly infringing on the ability of the agencies to fulfill their missions.

SPECIFIC EXEMPTIONS

Section 552a(k) would permit the head of any agency to exempt certain systems of records within his agency from some of the requirements of the legislation. The requirements from which these systems could be exempted are primarily those dealing with access by individuals to records about themselves. Only four categories of systems of records could be so excluded:

1. Information classified in the interest of national defense or foreign policy;

2. Investigatory material compiled for law enforcement purposes, except for information that is contained in criminal justice records (which are subject to section 552a(j)) and information that is open to public inspection under section 552 of this title, (the Freedom of Information Act);

3. Secret Service files maintained in connection with providing protective services to the President or other individuals; and

4. Records required by statute to be maintained and used solely as statistical research or reporting records.

Sound reasons of public policy justify exempting each of these groups of records from individual access.

1. In some cases, disclosure of classified information, even to the person to whom it pertains, could damage the national defense or foreign policy, for the information would no longer be subject to all the security controls it is properly subject to as classified matter.

2. Individual access to certain law enforcement files could impair investigations, particularly those which involve complex and continuing patterns of behavior. It could alert subjects of investigations that their activities are being scrutinized, and thus allow them time to take measures to prevent detection of illegal action or escape prosecution.

3. Access to Secret Service intelligence files on certain individuals would vitiate a critical part of Secret Service work which was specifically recommended by the Warren Commission that investigated the assassination of President Kennedy and funded by Congress.

4. Disclosure of statistical records in most instances would not provide any benefit to anyone, for these records do not have a direct effect on any given individual; it would, however, interfere with a legitimate, Congressionally-sanctioned activity.

As with systems of records which are exempted from virtually all requirements of the legislation by section 552a(j), the systems of records described in section (k) may be exempted from requirements only after the head of an agency promulgates rules which are open to public comment before they become effective. Also as with section (j) records, the Committee urges agencies maintaining section (k) records to open those documents to the individuals named in them insofar as such action would not impair the proper functioning of the agencies.

ARCHIVAL RECORDS

Section 552a(l) prescribes special provisions for records which are under the custody or control of the National Archives and Records Service, a constituent agency of the General Services Administration.

Paragraph (1) of this section deals with agency records accepted by the Administrator of General Services for storage, processing, and servicing which are now being provided by Federal Records Centers. These records are under the *control* of the agencies which deposited them; the National Archives and Records Service merely has *custody* of them while it is providing storage in Records Centers. Consequently, the paragraph states that these records shall, for the purposes of this section, be considered to be maintained by the agency which deposited them and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose any of these records except to the agency which maintains them or pursuant to rules established by that agency.

Paragraphs (2) and (3) deal with agency records pertaining to identifiable individuals which are transferred to the National Archives itself as records which have sufficient historical or other value to warrant their continued preservation by the United States Government. These records are under the actual *control* of the Archives; consequently, they shall, for the purposes of this section, be considered to be maintained by that agency.

Under paragraph (2), records which were transferred to the Archives *prior* to the effective date of this section shall not be subject to the provisions of the legislation. The Committee has written this exclusionary statement into the bill because it feels that requiring the Archives to reorganize large quantities of documents which are being used only for historical purposes would be expensive and would aid no one.

Under paragraph (3), records which are transferred to the Archives *after* the effective date shall be subject to most of the provisions of the bill. Since the records would already have been organized in conformity with the requirements of this section by the agency transferring them to the Archives, maintaining them in continued conformity with this law would not require any special effort. Permitting access to the records by individuals named in them would also be reasonable if access had been permitted by the agency which transferred the records to the Archives. (Insofar as a record could have been exempted from access under section 552a(j) or (k) before its transfer to the Archives, it could of course be similarly exempted after transfer by the Archivist of the United States.)

Records under the control of the Archives would not, however, be subject to the provisions of this law which permit changes in documents at the request of the individual named in them. A basic archival rule holds that archivists may not remove or amend information in any records placed in their custody. The principle of maintaining the integrity of records is considered one of the most important rules of professional conduct. It is important because historians quite properly want to learn the true condition of past government records when doing research; they frequently find the fact that a record was *inaccurate* is at least as important as the fact that a record was accurate.

The Committee believes that this rule is eminently reasonable and should not be breached even in the case of individually identifiable records. Once those documents are given to the Archives, they are no longer used to make any determination about any individual, so amendment of them would not aid anyone. Furthermore, the Archives has no way of knowing the true state of contested information, since it does not administer the program for which the data was collected; it cannot make judgments as to whether records should be altered.

ANNUAL REPORT

Section (m) provides that the President shall submit to the Speaker of the House of Representatives and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records that were exempted from the operative provisions of this law under the terms of section (j) or (k). Also to be included in the annual report would be the reasons for such exemptions and other information indicating efforts to comply with the law. It is hoped that all such information would be made public. If, however, the nature of any such exemption requires a security classification marking, it should be placed in a separate part of the report so as not to affect the remainder of the annual report.

TECHNICAL CHANGES

Section 4 of the bill makes necessary revisions of the chapter listing of chapter 5, title 5, United States Code to add this new section 552a —"Records about individuals".

EFFECTIVE DATE

Section 5 of the bill provides that it become effective on the 180th day following the date of enactment.

Cost Estimate

In compliance with clause 7 of rule XIII of the House of Representatives, the following statement is made relative to the cost which might be incurred in implementing this bill.

The Office of Management and Budget (OMB) estimates the annual cost of implementing this bill as between $200 million to $300 million

a year, with a one-time "start-up" cost of $100 million. Thus, the five-year estimate would range from $1.1 billion to $1.6 billion.

However, OMB made it clear that its estimates cannot have a higher degree of precision because of many imponderables, including possible savings off-sets. These problems were described in a letter from Mr. Robert H. Marik, Associate Director of OMB for Management and Operations, a copy of which may be found in the appendix of this report.

In the circumstances, the Committee concurs in the estimate of the Office of Management and Budget. The Committee also notes the Administration has circulated a proposed Executive order in the various agencies of the Government to carry out the objectives of this legislation. That Executive order was designed to be issued in the event Congress does not act. It is patterned very much after the House bill, H.R. 16373, now before you. The Office of Management and Budget has stated the cost of implementing this proposed Executive order would be approximately the same as the House bill. So the cost factor appears to be virtually academic. Our Government, subject to the President's final approval, intends to spend this money for this purpose whether we act or not. However, this is a congressional responsibility.

AGENCY VIEWS

See letter from OMB and Civil Service Commission, dated September 18, 1974, to Chairman Holifield.

EXECUTIVE OFFICE OF THE PRESIDENT,
OFFICE OF MANAGEMENT AND BUDGET,
Washington, D.C., October 2, 1974.

Hon. WILLIAM S. MOORHEAD,
Chairman, Foreign Operations and Government Information Subcommittee, Committee on Government Operations, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: This letter is intended to summarize our views with respect to H.R. 16373 which was recently ordered to be reported by the Committee on Government Operations.

Since time does not permit us to seek the view of all agencies concerned we are unable to speak for them. However, we have noted that this bill is in most respects consistent with earlier legislative proposals which were reviewed with those agencies.

We remain concerned, however, that the bill does not exempt from certain of its operative provisions, personnel testing and examination material and other personnel security and evaluation files, especially those containing information gathered under a pledge of confidentiality. Permitting unrestricted individual access to such records would seriously hamper agencies in evaluating the qualifications and reliability of Federal civilian, military, and contractor personnel.

With the exception of these provisions, we find the bill to be generally consistent with our views on this subject.

Sincerely,

ROBERT H. MARIK,
Associate Director for Management and Operations.

U.S. Civil Service Commission,
Washington, D.C., September 18, 1974.

Hon. Chet Holifield,
Chairman, Committee on Government Operations, House of Representatives, Washington, D.C.

Dear Mr. Chairman: The Civil Service Commission strongly urges that the Committee restore to H.R. 16373 exemptions which will enable the Commission to continue efficiently to carry out its responsibilities with respect to Federal employee management. The exemptions were in paragraphs (4) and (5) of the proposed section 552a(j) to title 5, United States Code, as added by section 3 of H.R. 16373. As introduced, these provisions would have exempted from the disclosure and access-to-records provisions of the legislation:

> (4) Investigatory material maintained for the purpose of determining initial or continued eligibility or qualification for Federal employment, military service, Federal contracts, or access to classified information; or
>
> (5) Material used for appointment, employment, or promotion in the Federal service.

The latter item while very broad was intended principally to protect materials used in civil service examinations.

With respect to investigative material, the Commission is authorized and directed, pursuant to 5 U.S.C. 3301 and 3302, to examine into the character and fitness of civil service applicants in order to determine their relative suitability for employment. These suitability determinations are essential to the maintenance of a high-caliber work force because they insure that from the standpoint of character and integrity, as well as of qualifications, we select the very best applicants for Government employment.

Our long experience in investigations indicates that those who give witness to the qualifications and integrity of others are ordinarily far more candid when the information is given under pledge of confidence than they are when they presumably are speaking for publication. And this experience is borne out whether the person who reports to us is a former employer, an associate, or a neighbor. Without an exemption similar to that stated in subsection (4) quoted above, we could not maintain the confidentiality of the information we receive or of its sources, with the result that we could not effectively perform the full reach of our statutory functions. In a word, we could not give adequate assurance that persons employed were in fact qualified from the standpoint of either competence or integrity.

With respect to examining material, the Commission must maintain the integrity of the competitive process which plays such an important part in the staffing of the competitive service. Obviously, in determining the relative ability of competitors for Federal positions, the Commission must use an examining process which is scrupulously fair to all who are concerned. If test questions and rating information is made available to the persons to whom they pertain, the Commission will be unable to control the dissemination of such information to others. Applicants, by learning the correct answers to the questions, could use the information to compromise the fairness of the entire testing system, and reduce to a shambles the open competitive examining

system we have worked so hard to establish. In order to protect our examinations from compromise, particularly when we use written tests, we currently follow procedures in which we compose tests of differing series of similar questions and this scrambling technique barely keeps us ahead of those who would exploit our tests for personal or commercial gain. Without an exemption for materials used in the examining process, we could not defend our tests against compromise. In addition, if the names and ratings of other applicants must be revealed to any requesting applicant, questions arise as to whether or not the rights of privacy of these other applicants have been violated.

We also believe that medical records of employees and applicants should not be generally available, even to the applicant or employee, when this information could be harmful to him. Our regulations provide for release of this information to the person requesting it only through a doctor of his choice. We believe that this procedure should be maintained.

Time has permitted only a brief discussion of the problems we anticipate if Commission operations, particularly those discussed above, are not exempted from the provisions of the bill. We strongly urge that the Committee consider the impact of the inclusion of all the records maintained by the Civil Service Commission in the disclosure and access provisions of this bill. We recommend that the Committee restore exemptions for the Commission, and for the military departments, which we understand have similar problems. We offer the following language to provide minimum protections for our operations:

"(4) investigatory and examining material maintained for the purpose of determining initial or continued eligibility or qualification for

"(A) Federal employment,

"(B) military service,

"(C) employment under Federal contracts,

"(D) access to classified information; or

"(5) medical information concerning a mental or other condition of a Federal employee or applicant for Federal employment of such a nature that a prudent physician would hesitate to inform the person suffering from the condition of its exact nature and probable outcome, except that this information will be disclosed to a licensed physician designated in writing by the individual for that purpose."

We believe that exemptions such as those stated immediately above will enable the Commission to continue to carry out its responsibilities for maintaining a superior Federal work force. We recognize our obligation to furnish to Federal employees and applicants for employment all information possible concerning them consistent with these responsibilities.

By Direction of the Commission:

Sincerely yours,

ROBERT E. HAMPTON,
Chairman.

Section-by-Section Analysis

The findings of the bill state that individual privacy is affected by the collection, maintenance and use of individually identifiable data by the Federal Government and that control of such systems of data is necessary to insure privacy.

The purpose of the act is to provide safeguards for the collection and use of such records, identify record systems, provide reasonable access by individuals to their records, and provide civil remedies for violations of its provisions.

Section (a) defines various terms used for the purposes of this act.

Section (b) prohibits dissemination of records outside the agency except when requested or permitted with prior written consent by the affected individual. Other exceptions are when it is used for a legitimate routine purpose defined under formal rulemaking; submitted to another governmental unit for a law enforcement activity authorized by statute upon written request; to the Census Bureau for activities pursuant to title 13, U.S.C.; for statistical use when provided in a non-individually identifiable form; pursuant to a showing of a compelling circumstance affecting the individual's health or safety and then only upon transmittal of notice to the individual; when transferred to the National Archives or provided to Congress.

Section (c) requires an accurate accounting of the fact and nature of any dissemination of a record, which accounting shall be retained for five years and be made available upon request to the affected individual. This section also requires that an agency inform others about any correction or notation of dispute disclosed to another agency within two years preceding the making of such correction on a record.

Section (d) requires an agency to grant access by an individual to his records for inspection and/or copying; permits individuals to request correction of records, and provides for an interagency review of refusals to correct upon request. This section also permits an individual to file a concise statement setting forth his reasons for disagreeing with an agency's refusal to amend the record, requires the agency to clearly note the disputed portion of the record, and permits the agency to include a rebuttal statement.

Section (e) enumerates agency requirements to inform individuals of their rights when supplying information and also requires annual publication in the *Federal Register* by each agency which maintains a record system the name and location of each system; the category of persons and records maintained in each system; use policies of each agency and the title and business address of the person responsible for such system.

It also prohibits any Federal agency from maintaining any record concerning the political or religious belief or activity on any individual unless expressly authorized by statute or the individual himself.

Section (f) also states that each agency shall under the Administrative Procedure Act set rules providing for access to requested records; describe routine uses of maintained records; establish proce-

dures for amending records and keeping them in a timely, relevant and accurate fashion; establish procedures for disclosing medical records to individuals; and may set fees for providing copies of requested records except that no fees shall be charged for search or review of records.

Section (g) provides a civil remedy for individuals who have been denied access to their records, or whose records have been kept or used in contravention of the requirements of the act and an adverse effect results. Suit may be brought in a district where the complainant resides, does business, where the records are located, or in the District of Columbia. The complainant may recover actual damages and costs and attorney fees if the agencies' infraction was willful, arbitrary, or capricious.

Section (h) provides that for the purposes of subsections relating to disclosure, access or civil remedies, a minor or an adjudged incompetent may be represented by his legal guardian.

Section (i) makes unlawful possession of or disclosure of individually identifiable information by a government employee punishable by a fine not to exceed $5,000 and also provides that any person who requests or obtains such a record by false pretenses is subject to a fine not to exceed $5,000.

Section (j) states that except as to certain agency conditions of disclosure and requirements, records determined under formal rulemaking maintained by the CIA and records maintained for law enforcement purposes are exempt from the provisions of the act.

Section (k) permits an agency head to exempt any record or system of records through formal rulemaking from the provisions of subsections relating to disclosure, accounting availability, access availability, and certain agency rules; records which are classified; are maintained for Secret Service protective purposes; or required by statute to be maintained solely for statistical reporting or research purposes.

Section (l) provides, among other things, that records accepted by the National Archives under section 3103 of title 44, U.S.C. shall be considered for the purposes of this act to be maintained by the depositing agency.

Section (m) provides for an annual report by the President listing the number of records contained in any system of records exempted under sections (i) and (j) and reasons for such exemptions.

Section 6 sets the effective date of the act at 180 days after enactment except for section (f), which becomes effective on the date of enactment.

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3 of Rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

TITLE 5, UNITED STATES CODE

* * * * * * *

CHAPTER 5—ADMINISTRATIVE PROCEDURE

SUBCHAPTER I—GENERAL PROVISIONS

SEC.
500. Administrative practice; general provisions.
501. Advertising practice; restrictions.
502. Administrative practice; Reserves and National Guardsmen.
503. Witness fees and allowances.

SUBCHAPTER II—ADMINISTRATIVE PROCEDURE

SEC.
551. Definitions.
552. Public information; agency rules, opinions, orders, records, and proceedings.
552a. Records about individuals.
553. Rule making.
554. Adjudications.
555. Ancillary matters.
556. Hearings; presiding employees; powers and duties; burden of proof; evidence; record as basis of decision.
557. Initial decisions; conclusiveness; review by agency; submissions by parties; contents of decisions; record.
558. Imposition of sanctions; determination of applications for licenses; suspension, revocation, and expiration of licenses.
559. Effect on other laws; effect of subsequent statute.

SUBCHAPTER III—ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

SEC.
571. Purpose.
572. Definitions.
573. Administrative Conference of the United States.
574. Powers and duties of the Conference.
575. Organization of the Conference.
576. Appropriations.

SUBCHAPTER I—GENERAL PROVISIONS

* * * * * * *

SUBCHAPTER II—ADMINISTRATIVE PROCEDURE

* * * * * * *

§ 552a. Records maintained on individuals

(a) DEFINITIONS.—For purposes of this section—

(1) the term "agency" means agency as defined in section 552(e) of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use, or disseminate;

(4) the term "record" means any collection or grouping of information about an individual that is maintained by an agency

and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual; and

(6) the term "statistical research or reporting record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13.

(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) for a routine use described in any rule promulgated under subsection (e)(2)(D) of this section;

(3) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(4) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(5) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

(6) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(7) pursuant to a showing of compelling circumstances affecting the health or safety of an individual, if upon the disclosure notification is transmitted to the last known address of the individual; or

(8) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee.

(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

(1) except for disclosures made under subsection (b)(1) of this section or disclosures to the public from records which by law or regulation are open to public inspection or copying, keep an accurate accounting of—

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b) (6) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency within two years preceding the making of the correction of the record of the individual, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section or for which no accounting of the disclosure is required.

(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him to review the record and have a copy made of all or any portion thereof in a form comprehensible to him;

(2) permit the individual to request amendment of a record pertaining to him and either—

(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(B) promptly inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

(3) permit any individual who disagrees with the refusal of the agency to amend his record to request review of the refusal by the official named in accordance with paragraph (2)(B) of this subsection; and if, after the review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency; and

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after

the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and, upon request, provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed.

(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

(1) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

(A) which Federal statute or regulation, if any, requires disclosure of the information;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) other purposes for which the information may be used, as published pursuant to paragraph (2)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(2) publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine purpose for which the records contained in the system are used or intended to be used, including the categories of users of the records for each such purpose;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; and

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content;

(3) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; and

(4) maintain no record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained.

(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means the head of the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection in a form available to the public at low cost.

(g)(1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d)(1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of the record and consequently a determination is made which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (j) or (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3) In any suit brought under the provisions of subsection (g)(1)(B) and (C) of this section in which the court determines that the

agency acted in a manner which was willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment of official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.

(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from any part of this section except subsections (b) and (e)(2)(A) through (F) if the system of records is—

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investiga-

93-699 O - 74 - 22

tors, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(2 (G) and (H), and (f) of this section if the system of records is—

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigating material compiled for law enforcement purposes, except to the extent that the material is within the scope of subsection (j)(2) of this section or is open to public inspection under the provisions of section 552(b)(7) of this title;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18; or

(4) required by statute to be maintained and used solely as statistical research or reporting records.

(l)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsections (c)(4); (d)(2), (3), and (4); (e) (1), (2)(H) and (3); (f)(4); (g)(1)(B) and (C), and (3).

(m) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

* * * * * * *

APPENDIX

Correspondence Regarding Cost Estimate

Executive Office of the President,
Office of Management and Budget,
Washington, D.C., September 19, 1974.

Hon. William S. Moorhead,
Chairman, Foreign Operations and Government Information Subcommittee, Committee on Government Operations, House of Representatives, Washington, D.C.

Dear Mr. Chairman: This letter is to confirm the essence of our discussions last evening in regard to the costs of implementing H.R. 16373, consistent with the amendments which we have proposed.

I would like to reiterate that it is extremely difficult to develop any reliable estimate of the cost of this legislation, because it plows new ground in areas where we have virtually no operating experience, and there are so many interdependent variables of unknown magnitude.

We have been working with the Executive Departments and Agencies since May to develop cost estimates in connection with the privacy provisions transmitted to you in our letter of June 19, 1974. Those efforts have not yielded firm estimates, but rather have underscored the difficulty which operating organizations are experiencing in attempting to quantify the costs involved. Some of the major imponderables we have encountered are:

There is considerable uncertainty, as confirmed by Senator Ervin's study, about the total number and magnitude of personal data systems currently being maintained by various government agencies.

The disincentives to collecting personal data inherent in this legislation will probably result in a reduction in the amount of data collected and stored in various agency systems, and possibly the elimination of some existing systems. However, the disincentives to transferring personal data between agencies will have the countereffect of stimulating more systems to meet the unique needs of a given agency. There is considerable uncertainty about the offsetting effects of these two factors.

It is difficult to predict the extent to which individuals will exercise the rights afforded to them by this bill. For example, how many people will inquire whether they are included in specific agency systems and how many will request copies of their data or modifications of the data maintained about them.

There is uncertainty about the extent to which reduced efficiencies in computer utilization resulting from the introduction of safeguards will be offset by technological improvements being developed by industry.

For the foregoing reasons, our estimate cannot have a high degree of precision. Within those limitations, we believe the costs of implementing H.R. 16373 will be on the order of $200 to $300 million per year over the next four to five years, with an additional one-time start-up cost of about $100 million, which would be expended within the first two years. As previously indicated, there are some possible offsetting factors which could reduce the actual cost. However, we believe that a year's operating experience will be necessary before greater precision in the cost estimates can be achieved.

There is no doubt that privacy safeguards of the type envisioned in this bill will result in added costs of operations. We have appreciated the concern of the Subcommittee about costs, and their continued efforts to minimize the cost impact as the bill has evolved. Our estimate of the costs associated with the current draft are less than half of the costs which we had estimated for earlier drafts which were under consideration.

Sincerely,

ROBERT H. MARIK,
Associate Director for Management and Operations.

ADDITIONAL VIEWS OF HON. BELLA S. ABZUG (CONCURRED IN BY HON. JOHN E. MOSS, HON. DANTE B. FASCELL, HON. BENJAMIN S. ROSENTHAL, HON. JOHN C. CULVER, HON. JOHN CONYERS, JR., HON. JAMES V. STANTON, HON. CARDISS COLLINS, HON. JOHN L. BURTON, AND HON. GILBERT GUDE)

H.R. 16373 is the product of many months of hard work by the members and staff of the Foreign Operations and Government Information Subcommittee. During the course of these months, all of us who have been involved in the process of writing this legislation have learned a great deal about the complex concept of "privacy". Fortunately, as a result of this learning experience, instigated by the introduction of several excellent privacy bills, the bill which the full Government Operations Committee reported out on September 24th represents an improvement in a number of ways, both organizationally and substantively, over earlier drafts of this bill. There is still room for much improvement, however. We feel that there are several additions and changes which must be made to strengthen the bill. In view of the difficulty of maintaining a quorum and the pressure of time, these could not be effectively considered at the full committee meeting, but will be presented when the bill reaches the floor.

There are three basic weaknesses in the bill: the numerous and unjustified exemption provisions, the failure to provide either liquidated or punitive damages, and the lack of any administrative mechanism to oversee the implementation of the bill.

EXEMPTIONS

We start with the premise that exemptions from the provisions of this bill and of any bill designed to protect individual rights of privacy are justified only in the face of overwhelming societal interests. Never should economy or efficiency or administrative convenience be used to justify the exemption from or modification of any of the safeguard requirements set forth in this bill. Moreover, when exemptions must be made, they must be defined in very specific terms.

The Committee bill sets forth six categories in which exemptions may be made: (1) records maintained by the C.I.A., (2) certain records maintained by criminal law enforcement agencies, (3) information affecting national security within the scope of Section 552(b)(1) of Title 5, U.S. Code, (4) investigatory material compiled for law enforcement purposes, both criminal and civil, (5) records maintained in connection with certain protective services, and (6) records required by statute to be maintained and used solely for statistical research or operating. Within any of these categories the bill delegates

to the heads of the various Federal agencies the task of balancing individual rights against societal interests and of deciding which is paramount. Few guidelines have been set forth, however, to enable agency heads to perform this rather delicate task.

We feel that there are, at most, only three areas where societal interest can be paramount to the individual rights provided by this bill: (1) where granting an individual access to his or her records would seriously damage national defense or foreign policy; (2) where such access would interfere with an active criminal prosecution; and (3) where records are required by law to be maintained for statistical research or reporting purposes and are not, in fact, used to make determinations about identifiable individuals. By narrowing the exemption categories and defining them in specific terms related to the use of records rather than to the agency maintaining them, Congress could provide agency heads with standards to meet in exercising their rulemaking authority to grant exemptions. Only in this way can we be assured that the constitutional rights of individuals will be protected and will not be sacrificed to administrative discretion, expediency or whim.

DAMAGES

The bill in its present form contains provisions for the assessment of actual damages, court costs, and attorneys' fees in cases where an agency is found to be in violation of the law. A provision allowing court assessment of punitive damages, which is contained in the Senate bill (S. 3418), was stricken in full committee. We feel strongly that this provision should be restored to the bill. Actual damages resulting from an agency's misconduct will, in most cases, be difficult to prove and this will often effectively preclude an adequate remedy at law. Moreover, if we are concerned with effectively deterring the willful, arbitrary, or capricious disclosure or transfer of protected records, a provision permitting a court to assess punitive damages or, at the very least, liquidated damages is essential.

THE NEED FOR AN ADMINISTRATIVE AGENCY

Unlike the Senate bill, H.R. 16373 contains no provision for the establishment of an administrative body to oversee the implementation of this legislation. We recognize the fact that some of our colleagues feel it is wiser to wait and see how Federal agencies respond to privacy legislation before establishing any oversight mechanism. No one, however, wants to repeat the experience of the Freedom of Information Act in holding out rights to individuals but providing them only with the costly and cumbersome mechanism of a judicial remedy. Therefore, we would amend the bill to provide for the establishment of an administrative body to mediate conflicts between agencies and individuals, to investigate complaints, hold hearings, and make findings of fact.

We would be more than naive if we failed to recognize that individual Federal agencies cannot be expected to take an aggressive role in enforcing privacy legislation. Enforcement of the provisions of this bill will be secondary to each agency's legislative mandate and will, of

necessity, cause additional expense and administrative inconvenience. Only by providing a separate administrative agency with authority for implementing this legislation and coordinating the privacy programs of the various Federal agencies can we be assured of uniform, effective enforcement of the rights guaranteed by this bill.

BELLA S. ABZUG,
JOHN E. MOSS,
JAMES V. STANTON,
GILBERT GUDE,
JOHN BURTON,
DANTE B. FASCELL,
JOHN CULVER,
CARDISS COLLINS,
BENJAMIN ROSENTHAL,
JOHN CONYERS, JR.,

ADDITIONAL VIEWS OF HON. JOHN N. ERLENBORN (CONCURRED IN BY HON. PAUL N. McCLOSKEY, JR., HON. SAM STEIGER, HON. CHARLES THONE, AND HON. ROBERT P. HANRAHAN)

The Committee states in this report, "H.R. 16373 attempts to strike that delicate balance between two fundamental and conflicting needs—on the one hand, that of the individual American for a maximum degree of privacy over personal information he furnishes his government, and on the other, that of the government for information about individual citizens which it finds necessary to carry out its legitimate functions."

We commend the members of the Committee for keeping this objective in mind when writing the bill. We believe that they have failed to follow it, however, with regard to two important kinds of information. Should the bill reach the Floor of the House, we shall therefore offer an amendment to add these two kinds of information to the categories which may be exempted from the provisions of the bill which permit individuals to have access to records maintained about them. The two, which we urge should be made items (5) and (6) in subsection 552a(k), are:

—investigatory material compiled solely for the purpose of determining initial or continuing eligibility or qualification for Federal employment, military service, Federal contracts, or access to classified information; and

—testing or examination material used for appointment, employment, or promotion in the Federal service.

With regard to these types of records, individual access would impair the carrying out of legitimate functions of government. Those functions are so important that the principle of access to records should be put aside here.

INVESTIGATORY MATERIAL

Government agencies must be able to choose the best applicants for employment and military service if they are to fulfill their missions most effectively. They must be able to select the best contractors to perform additional necessary work. They must be especially careful in certifying which individuals may view information the disclosure of which could damage, in some cases severely, the national defense or foreign policy of the United States.

To have the ability to make these important judgments, agencies need honest opinions about the people they are investigating. The Civil Service Commission, speaking for all agencies, has testified that "Our long experience in investigations indicates that those who give

witness to the qualifications and integrity of others are ordinarily far more candid when the information is given under pledge of confidence than they are when they presumably are speakng for publication." If the information were to be available to the individuals to whom it pertains, the government could not make a pledge of confidence to the people whom it solicits for personal opinions. Future information would not be forthcoming. Past information would be revealed, violating the privacy of the people who gave it. This would be a most unfortunate result.

TESTING MATERIAL

The military services and the Civil Service Commission test applicants to determine eligibility and ratings for military placement and on merit system schedules. Individuals are informed of their scores on these tests and how the scores compare with those of other people who took the same examinations. Revealing the test questions and answers in addition would not help the individuals in any way; it certainly would not protect their privacy. This disclosure would have only one result: the examination material would be made public. As a result, to make all tests fair, examining agencies would have to develop a new version of each test for each occasion on which it would be given. This would be a needless expense.

In short, we seek not the invasion of privacy but the furtherance of important government objectives in areas where privacy considerations do not weigh heavily. We support most emphatically the protection of personal privacy, and offer this amendment only to improve a bill which is directed toward that end.

JOHN N. ERLENBORN,
PAUL N. MCCLOSKEY, Jr.,
SAM STEIGER,
CHARLES THONE,
ROBERT P. HANRAHAN.

93D CONGRESS
2D SESSION

S. 3418

AN ACT

To establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I—PRIVACY PROTECTION COMMISSION

ESTABLISHMENT OF COMMISSION

SEC. 101. (a) There is established as an independent agency of the executive branch of the Government the Privacy Protection Commission.

(b) (1) The Commission shall be composed of five members who shall be appointed by the President, by and

★

with the advice and consent of the Senate, from among members of the public at large who, by reason of their knowledge and expertise in any of the following areas: civil rights and liberties, law, social sciences, and computer technology, business, and State and local government, are well qualified for service on the Commission and who are not otherwise officers or employees of the United States. Not more than three of the members of the Commission shall be adherents of the same political party.

(2) One of the Commissioners shall be appointed Chairman by the President.

(3) A Commissioner appointed as Chairman shall serve as Chairman until the expiration of his term as a Commissioner of the Commission (except that he may continue to serve as Chairman for so long as he remains a Commissioner and his successor as Chairman has not taken office). An individual may be appointed as a Commissioner at the same time he is appointed Chairman.

(c) The Chairman shall preside at all meetings of the Commission and a quorum for the transaction of business shall consist of at least three members present (but the Chairman may designate an Acting Chairman who may preside in the absence of the Chairman). Each member of the Commission, including the Chairman, shall have equal respon-

sibility and authority in all decisions and actions of the Commission, shall have full access to all information relating to the performance of his duties or responsibilities, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or Acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, persons, or the public, and, on behalf of the Commission, shall see to the faithful execution of the policies and decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

(d) Each Commissioner shall be compensated at the rate provided for under section 5314 of title 5 of the United States Code, relating to level IV of the Executive Schedule.

(e) Commissioners shall serve for terms of three years. No Commissioner may serve more than two terms. Vacancies in the membership of the Commission shall be filled in the same manner in which the original appointment was made.

(f) Vacancies in the membership of the Commission, as long as there are three Commissioners in office, shall not impair the power of the Commission to execute the functions and powers of the Commission.

(g) The members of the Commission shall not engage in any other employment during their tenure as members of the Commission.

(h) (1) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress.

(2) Whenever the Commission submits any legislative recomendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress.

PERSONNEL OF THE COMMISSION

SEC. 102. (a) (1) The Commission shall appoint an Executive Director who shall perform such duties as the Commission may determine. Such appointment may be made without regard to the provisions of title 5, United States Code.

(2) The Executive Director shall be compensated at a

rate not in excess of maximum rate for GS–18 of the General Schedule under section 5332 of title 5, United States Code.

(b) The Commission is authorized to appoint and fix the compensation of such officers and employees, and prescribe their functions and duties, as may be necessary to carry out the provisions of this Act.

(c) The Commission may obtain the services of experts and consultants in accordance with the provisions of section 3109 of title 5, United States Code.

FUNCTIONS OF THE COMMISSION

SEC. 103. (a) The Commission shall—

(1) publish annually a United States Directory of Information Systems containing the information specified to provide notice under section 201 (c) (3) of this Act for each information system subject to the provisions of this Act and a listing of all statutes which require the collection of such information by a Federal agency;

(2) investigate, determine, and report any violation of any provision of this Act (or any regulation adopted pursuant thereto) to the President, the Attorney General, the Congress, and the General Services Administration where the duties of that agency are involved, and to the Comptroller General when it deems appropriate; and

(3) develop model guidelines for the implementation

of this Act and assist Federal agencies in preparing regulations and meeting technical and administrative requirements of this Act.

(b) Upon receipt of any report required of a Federal agency describing (1) any proposed information system or data bank, or (2) any significant expansion of an existing information system or data bank, integration of files, programs for records linkage within or among agencies, or centralization of resources and facilities for data processing, the Commission shall—

(A) review such report to determine (i) the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the confidentiality of information relating to such individuals, and (ii) its effect on the preservation of the constitutional principles of federalism and separation of powers; and

(B) submit findings and make recommendations to the President, Congress, and the General Services Administration concerning the need for legislative authorization and administrative action relative to any such proposed activity in order to meet the purposes and requirements of this Act.

(c) After receipt of any report required under subsection (b), if the Commission determines and reports to the

Congress that a proposal to establish or modify a data bank or information system does not comply with the standards established by or pursuant to this Act, the Federal agency submitting such report shall not proceed to establish or modify any such data bank or information system for a period of sixty days from the date of receipt of notice from the Commission that such data bank or system does not comply with such standards.

(d) In addition to its other functions the Commission shall—

(1) to the fullest extent practicable, consult with the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out the provisions of this Act and in conducting the study required by section 106 of this Act;

(2) perform or cause to be performed such research activities as may be necessary to implement title II of this Act, and to assist Federal agencies in complying with the requirements of such title;

(3) determine what specific categories of information should be prohibited by statute from collection by Federal agencies on the basis that the collection of such information would violate an individual's right of privacy; and

(4) prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation.

CONFIDENTIALITY OF INFORMATION

SEC. 104. (a) Each department, agency, and instrumentality of the executive branch of the Government, including each independent agency, shall furnish to the Commission, upon request made by the Chairman, such data, reports, and other information as the Commission deems necessary to carry out its functions under this Act.

(b) In carrying out its functions and exercising its powers under this Act, the Commission may accept from any Federal agency or other person any identifiable personal data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall provide appropriate safeguards to insure that the confidentiality of such information is maintained and that upon completion of the purpose for which such information is required it is destroyed or returned to the agency or person from which it is obtained, as appropriate.

63-619 O - 76 - 23

POWERS OF THE COMMISSION

SEC. 105. (a) (1) The Commission may, in carrying out its functions under this Act, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Commission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2) In case of disobedience to a subpena issued under paragraph (1) of this subsection, the Commission may invoke the aid of any district court of the United States in requiring compliance with such subpena. Any district court of the United States within the jurisdiction where such person is found or transacts business may, in case of contumacy or refusal to obey a subpena issued by the Commission, issue an order requiring such person to appear and testify, to produce such books, records, papers, correspondence, and

documents, and any failure to obey the order of the court shall be punished by the court as a contempt thereof.

(3) Appearances by the Commission under this Act shall be in its own name. The Commission shall be represented by attorneys designated by it.

(4) Section 6001(1) of title 18, United States Code, is amended by inserting immediately after "Securities and Exchange Commission," the following: "the Privacy Protection Commission,".

(b) The Commission may delegate any of its functions to such officers and employees of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(c) In order to carry out the provisions of this Act, the Commission is authorized—

(1) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(2) to adopt, amend, and repeal interpretative rules for the implementation of the rights, standards, and safeguards provided under this Act;

(3) to enter into contracts or other arrangements or modifications thereof, with any government, any agency or department of the United States, or with any person, firm, association, or corporation, and such contracts or

other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(4) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529);

(5) receive complaints of violations of this Act and regulations adopted pursuant thereto; and

(6) to take such other action as may be necessary to carry out the provisions of this Act.

COMMISSION STUDY OF OTHER GOVERNMENTAL AND PRIVATE ORGANIZATIONS

SEC. 106. (a) (1) The Commission shall make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information, and to determine the extent to which those standards and procedures achieve the purposes of this Act.

(2) The Commission periodically shall report its findings to the President and the Congress and shall complete

the study required by this section not later than three years from the date this Act becomes effective.

(3) The Commission shall recommend to the President and the Congress the extent, if any, to which the requirements and principles of this Act should be applied to the information practices of those organizations by legislation, administrative action, or by voluntary adoption of such requirements and principles. In addition, it shall submit such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

(b) (1) In the course of such study and in its reports, the Commission shall examine and analyze—

(A) interstate transfer of information about individuals which is being undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to

identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the implied or explicitly recognized confidentiality of such information.

(2) The Commission shall include in its examination information activities in the following areas: medical, insurance, education, employment and personnel, credit, banking and financial institutions, credit bureaus, the commercial reporting industry, cable television and other telecommunications media, travel, hotel, and entertainment reservations, and electronic check processing. The Commission may study such other information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

(3) In conducting the study, the Commission shall—

(A) determine what laws, Executive orders, regu-

lations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) conduct a thorough examination of standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information;

(D) to the maximum extent practicable, collect and utilize findings, reports, and recommendations of major governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission; and

(E) receive and review complaints with respect to any matter under study by the Commission which may be submitted by any person.

REPORTS

SEC. 107. The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this Act.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, INTELLIGENCE, STATISTICAL-REPORTING, AND RESEARCH PURPOSES

SEC. 201. (a) Each Federal agency shall—

(1) collect, solicit, and maintain only such personal information as is relevant and necessary to accomplish a statutory purpose of the agency;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs; and

(3) inform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, will result from nondisclosure, and what rules of confidentiality will govern the information.

(b) Each Federal agency that maintains an information system or file shall, with respect to each such system or file—

(1) insure that personal information maintained in

the system or file is accurate, complete, timely, and relevant to the purpose for which it is collected or maintained by the agency at the time any access is granted to the file, material is added to or taken from the file, or at any time it is used to make a determination affecting the subject of the file;

(2) refrain from disclosing any such personal information within the agency other than to officers or employees who have a need for such personal information in the performance of their duties for the agency;

(3) maintain a list of all categories of persons authorized to have regular access to personal information in the system or file;

(4) maintain an accurate accounting of the date, nature, and purpose of all other access granted to the system or file, and all other disclosures of personal information made to any person outside the agency, or to another agency, including the name and address of the person or other agency to whom disclosure was made or access was granted, except as provided by section 202 (b) of this Act;

(5) establish rules of conduct and notify and instruct each person involved in the design, development, operation, or maintenance of the system or file, or the collection, use, maintenance, or dissemination of infor-

mation about an individual, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance;

(6) establish appropriate administrative, technical and physical safeguards to insure the security of the information system and confidentiality of personal information and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom personal information is maintained; and

(7) establish no program for the purpose of collecting or maintaining information describing how individuals exercise rights guaranteed by the first amendment unless the head of the agency specifically determines that such information is relevant and necessary to carry out a statutory purpose of the agency.

(c) Any Federal agency that maintains an information system or file shall—

(1) make available for distribution upon the request of any person a statement of the existence and character of each such system or file;

(2) on the date on which this Act becomes effective and annually thereafter, notify the Commission and give public notice of the existence and character of each ex-

isting system or file simultaneously, and cause such notice to be published in the Federal Register; and

(3) include in such notices at least the following information:

(A) name and location of the system or file;

(B) nature and purposes of the system or file;

(C) categories of individuals on whom personal information is maintained and categories of personal information generally maintained in the system or file, including the nature of the information and the approximate number of individuals on whom information is maintained;

(D) the confidentiality requirements and the extent to which access controls apply to such information;

(E) categories of sources of such personal information;

(F) the Federal agency's policies and practices regarding implementation of sections 201 and 202 of this Act, information storage, duration of retention of information, and elimination of such information from the system or file;

(G) uses made by the agency of the personal information contained in the system or file;

(H) identity of other agencies and categories of

persons to whom disclosures of personal information are made, or to whom access to the system or file may be granted, together with the purposes therefor and the administrative constraints, if any, on such disclosures and access, including any such constraints on redisclosure;

(I) procedures whereby an individual can (i) be informed if the system or file contains personal information pertaining to himself or herself, (ii) gain access to such information, and (iii) contest the accuracy, completeness, timeliness, relevance, and necessity for retention of the personal information; and

(J) name, title, official address, and telephone number of the officer immediately responsible for the system or file.

(d) (1) Each Federal agency that maintains an information system or file shall assure to an individual upon request the following rights:

(A) to be informed of the existence of any personal information pertaining to that individual;

(B) to have full access to and right to inspect the personal information in a form comprehensible to the individual;

(C) to know the names of all recipients of informa-

tion about such individual including the recipient organization and its relationship to the system or file, and the purpose and date when distributed, unless such information is not required to be maintained pursuant to this Act;

(D) to know the sources of personal information (i) unless the confidentiality of any such source is required by statute, then the right to know the nature of such source; or (ii) unless investigative material used to determine the suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, is compiled by a Federal agency in pursuit of an authorized investigative responsibility, and in the course of compiling such materials, information prejudicial to the subject of the investigation is revealed through a source who furnishes such information to the Government under the express provision that the identity of the source will be held in confidence, and where the disclosure of such information would identify and be prejudicial to the rights of the confidential source, then the right to know the nature of such information and to examine that information if it is found to be material or relevant to an administrative or judicial proceeding by a Federal judge or Federal administrative officer: *Provided*, That investi-

gative material shall not be made available to promotion boards which are empowered to promote or advance individuals in Federal employment, except when the appointment would be from a noncritical to a critical security position;

(E) to be accompanied by a person chosen by the individual inspecting the information, except that an agency or other person may require the individual to furnish a written statement authorizing discussion of that individual's file in the person's presence;

(F) to receive such required disclosures and at reasonable standard charges for document duplication, in person or by mail, if upon written request, with proper identification; and

(G) to be completely informed about the uses and disclosures made of any such information contained in any such system or file except those uses and disclosures made pursuant to law or regulation permitting public inspection or copying.

(2) Upon receiving notice that an individual wishes to challenge, correct, or explain any personal information about him in a system or file, such Federal agency shall comply promptly with the following minimum requirements:

(A) investigate and record the current status of the personal information;

(B) correct or eliminate any information that is found to be incomplete, inaccurate, not relevant to a statutory purpose of the agency, not timely or necessary to be retained, or which can no longer be verified;

(C) accept and include in the record of such information, if the investigation does not resolve the dispute, any statement of reasonable length provided by the individual setting forth his position on the disputed information;

(D) in any subsequent dissemination or use of the disputed information, clearly report the challenge and supply any supplemental statement filed by the individual;

(E) at the request of such individual, following any correction or elimination of challenged information, inform past recipients of its elimination or correction; and

(F) not later than sixty days after receipt of notice from an individual making a request concerning personal information, make a determination with respect to such request and notify the individual of the determination and of the individual's right to a hearing before an official of the agency which shall if requested by the individual, be conducted as follows:

(i) such hearing shall be conducted in an ex-

peditious manner to resolve the dispute promptly and shall be held within thirty days of the request and, unless the individual requests a formal hearing, shall be conducted on an informal basis, except that the individual may appear with counsel, present evidence, and examine and cross-examine witnesses;

(ii) any record found after such a hearing to be incomplete, inaccurate, not relevant, not timely nor necessary to be retained, or which can no longer be verified, shall within thirty days of the date of such findings be appropriately modified or purged; and

(iii) the action or inaction of any agency on a request to review and challenge personal data in its possession as provided by this section shall be reviewable de novo by the appropriate United States district court.

An agency may, for good cause, extend the time for making a determination under this subparagraph. The individual affected by such an extension shall be given notice of the extension and the reason therefore.

(e) When a Federal agency provides by a contract, grant, or agreement for, and the specific creation or substantial alteration, or the operation by or on behalf of the agency of an information system or file and the primary

purpose of the grant, contract, or agreement is the creation, substantial alteration, or the operation by or on behalf of the agency of such an information system or file, the agency shall, consistent with its authority, cause the requirements of subsections (a), (b), (c), and (d) to be applied to such system or file. In cases when contractors and grantees or parties to an agreement are public agencies of States or the District of Columbia or public agencies of political subdivisions of States, the requirements of subsections (a), (b), (c), and (d) shall be deemed to have been met if the Federal agency determines that the State or the District of Columbia or public agencies of political subdivisions of the State have adopted legislation or regulations which impose similar requirements.

(f) (1) Any Federal agency maintaining or proposing to establish a personal information system or file shall prepare and submit a report to the Commission, the General Services Administration, and to the Congress on proposed data banks and information systems or files, the proposed significant expansion of existing data banks and information systems or files, integration of files, programs for records linkage within or among agencies, or centralization of resources and facilities for data processing, which report shall include—

(A) the effects of such proposals on the rights,

benefits, and privileges of the individuals on whom personal information is maintained;

(B) a statement of the software and hardware features which would be required to protect security of the system or file and confidentiality of information;

(C) the steps taken by the agency to acquire such features in their systems, including description of consultations with representatives of the National Bureau of Standards; and

(D) a description of changes in existing interagency or intergovernmental relationships in matters involving the collection, processing, sharing, exchange, and dissemination of personal information.

(2) The Federal agency shall not proceed to implement such proposal for a period of sixty days from date of receipt of notice from the Commission that the proposal does not comply with the standards established under or pursuant to this Act.

(g) Each Federal agency covered by this Act which maintains an information system or file shall make reasonable efforts to serve advance notice on an individual before any personal information on such individual is made available to any person under compulsory legal process.

(h) No person may condition the granting or withholding of any right, privilege, or benefit, or make as a con-

dition of employment the securing by any individual of any information which such individual may obtain through the exercise of any right secured under the provisions of this section.

DISCLOSURE OF INFORMATION

SEC. 202. (a) No Federal agency shall disseminate personal information unless—

(1) it has made written request to the individual who is the subject of the information and obtained his written consent;

(2) the recipient of the personal information has adopted rules in conformity with this Act for maintaining the security of its information system and files and the confidentiality of personal information contained therein; and

(3) the information is to be used only for the purposes set forth by the sender pursuant to the requirements for notice under this Act.

(b) Section 202 (a) (1) shall not apply when disclosure would be—

(1) to those officers and employees of that agency who have a need for such information in ordinary course of the performance of their duties;

(2) to the Bureau of the Census for purposes of planning or carrying out a census or survey pursuant

to the provisions of title 13, United States Code: *Provided*, That such personal information is transferred or disseminated in a form not individually identifiable.

(3) where the agency determines that the recipient of such information has provided advance adequate written assurance that the information will be used solely as a statistical reporting or research record, and is to be transferred in a form that is not individually identifiable; or

(4) pursuant to a showing of compelling circumstances affecting health or safety of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.

(c) Section 201 (b) (4) and paragraphs (1), (2), and (3) of subsection (a) of this section shall not apply when disclosure would be to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office. Nothing in this Act shall impair access by the Comptroller General, or any of his authorized representatives, to records maintained by an agency, including records of personal information, in the course of performance of such duties.

(d) (1) Nothing in this section shall be construed to limit the efforts of the Government pursuant to the provisions of chapter 35, title 44 of the United States Code (commonly

known as the Federal Reports Act) or any other statute, to reduce the burden on citizens of collecting information by means of combining or eliminating unnecessary reports, questionnaires, or requests for information.

(2) Nothing in this section shall be construed to affect restrictions on the exchange of information between agencies as required by chapter 35, title 44 of the United States Code (commonly known as the Federal Reports Act).

(e) Subsection (a) (1) of this section shall not apply when disclosure would be to another agency or to an instrumentality of any governmental jurisdiction for a law enforcement activity if such activity is authorized by statute and if the head of such agency or instrumentality has made a written request to or has an agreement with the agency which maintains the system or file specifying the particular portion of the information desired and the law enforcement activity for which the information is sought.

EXEMPTIONS

SEC. 203. (a) The provisions of section 201 (c) (3) (E), (d), and section 202, shall not apply to any personal information contained in any information system or file if the head of the Federal agency determines, in accordance with the provisions of this section, that the application of the provisions of any of such sections would seriously damage national defense or foreign policy or where the appli-

cation of any of such provisions would seriously damage or impede the purpose for which the information is maintained.

(b) The provisions of section 201(d) and section 202 shall not apply to law enforcement intelligence information or investigative information if the head of the Federal agency determines, in accordance with the provisions of any of such sections would seriously damage or impede the purpose for which the information is maintained: *Provided*, That investigatory records shall be exempted only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trail or an impartial adjudication, (C) disclose the identity of a confidential source, and in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source, (E) disclose confidential investigative techniques and procedures which are not otherwise generally known outside the agency, or (F) endangers the life or physical safety of law enforcement personnel: *Provided further*, That investigative information may not be exempted under this section where such information has been maintained for a period longer than is necessary to commence criminal prosecution. Nothing in this Act shall prohibit the disclosure of

such investigative information to a party in litigation where required by statute or court rule.

(c) (1) A determination to exempt any such system, file, or information may be made by the head of any such agency in accordance with the requirements of notice, publication, and hearing contained in sections 553 (b), (c), and (e), 556, and 557 of title 5, United States Code. In giving notice of an intent to exempt any such system, file, or information, the head of such agency shall specify the nature and purpose of the system, file, or information to be exempted.

(2) Whenever any Federal agency undertakes to exempt any information system, file, or information from the provisions of this Act, the head of such Federal agency shall promptly notify the Commission of its intent and afford the Commission opportunity to comment.

(3) The exception contained in section 553 (d) of title 5, United States Code (allowing less than thirty days' notice), shall not apply in any determination made or any proceeding conducted under this section.

ARCHIVAL RECORDS

SEC. 204. (a) Federal agency records which are accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44, United States Code, shall, for the purposes of this

section, be considered to be maintained by the agency which deposited the records and shall be subject to the provisions of this Act. The Administrator of General Services shall not disclose such records, or any information therein, except to the agency which maintains the records or pursuant to rules established by that agency.

(b) Federal agency records pertaining to identifiable individuals which were transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government shall for the purposes of this Act, be considered to be maintained by the National Archives and shall not be subject to the provisions of this Act except section 201(b) (5) and (6).

(c) The National Archives shall, on the date on which this Act becomes effective and annually thereafter, notify the Commission and give public notice of the existence and character of the information systems and files which it maintains, and cause such notice to be published in the Federal Register. Such notice shall include at least the information specified under section 201(c) (3) (A), (B), (D), (E), (F), (G), (I), and (J).

EXCEPTIONS

SEC. 205. (a) No officer or employee of the executive branch of the Government shall rely on any exemption in

subchapter II of chapter 5 of title 5 of the United States Code (commonly known as the Freedom of Information Act) to withhold information relating to an individual otherwise accessible to an individual under this Act.

(b) Nothing in this Act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder.

(c) The provisions of section 201 (d) (1) of this Act shall not apply to records collected or furnished and used by the Bureau of the Census solely for statistical purposes or as authorized by section 8 of title 13 of the United States Code: *Provided*, That such personal information is transferred or disseminated in a form not individually identifiable.

(d) The provisions of this Act shall not require the disclosure of testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service if the disclosure of such material would compromise the objectivity or fairness of the testing or examination process.

(e) The provisions of this Act, with the exception of sections 201 (a) (2), 201 (b) (2), (3), (4), (5), (6), and (7), 201 (c) (2), 201 (c) (3) (A), (B), (D), and (F), and 202 (a) (2) and (3) shall not apply to foreign intelligence information systems or to systems of personal

information involving intelligence sources and methods designed for protection from unauthorized disclosure pursuant to 50 U.S.C.A. 403.

MAILING LISTS

SEC. 206. (a) An individual's name and address may not be sold or rented by a Federal agency unless such action is specifically authorized by law. This provision shall not be construed to require the confidentiality of names and addresses otherwise permitted to be made public.

(b) Upon written request of any individual, any person engaged in interstate commerce who maintains a mailing list shall remove the individual's name and address from such list.

REGULATIONS

SEC. 207. Each Federal agency subject to the provisions of this Act shall, not later than six months after the date on which this Act becomes effective, promulgate regulations to implement the standards, safeguards, and access requirements of this title and such other regulations as may be necessary to implement the requirements of this Act.

TITLE III—MISCELLANEOUS

DEFINITIONS

SEC. 301. As used in this Act—

(1) the term "Commission" means the Privacy Protection Commission;

(2) the term "personal information" means any information that identifies or describes any characteristic of an individual, including, but not limited to, his education, financial transactions, medical history, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

(3) the term "individual" means a citizen of the United States or an alien lawfully admitted through permanent residence;

(4) the term "information system" means the total components and operations, whether automated or manual, by which personal information, including name or identifier, is collected, stored, processed, handled, or disseminated by an agency;

(5) the term "file" means a record or series of records containing personal information about individuals which may be maintained within an information system;

(6) the term "data bank" means a file or series of files pertaining to individuals;

(7) the term "Federal agency" means any department, agency, instrumentality, or establishment in the

executive branch of the Government of the United States and includes any officer or employee thereof;

(8) the term "investigative information" means information associated with an identifiable individual compiled by—

(A) an agency in the course of conducting a criminal investigation of a specific criminal act where such investigation is pursuant to a statutory function of the agency. Such information may pertain to that criminal act and be derived from reports of informants and investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically and expressly required by State or Federal statute to be made public; or

(B) by an agency with regulatory jurisdiction which is not a law enforcement agency in the course of conducting an investigation of specific activity which falls within the agency's regulatory jurisdiction. For the purposes of this paragraph, an "agency with regulatory jurisdiction" is an agency which is empowered to enforce any Federal statute

or regulation, the violation of which subjects the violator to criminal or civil penalties;

(9) the term "law enforcement intelligence information" means information associated with an identifiable individual compiled by a law enforcement agency in the course of conducting an investigation of an individual in anticipation that he may commit a specific criminal act, including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically by incident and expressly required by State or Federal statute to be made public;

(10) the term "criminal history information" means information on an individual consisting of notations of arrests, detentions, indictments, informations, or other formal criminal charges and any disposition arising from those arrests, detentions, indictments, informations, or charges. The term shall not include an original book of entry or police blotter maintained by a law enforcement agency at the place of an original arrest or place of detention, indexed chronologically and required to

be made public, nor shall it include court records of public criminal proceedings indexed chronologically; and

(11) the term "law enforcement agency" means an agency whose employees or agents are empowered by State or Federal law to make arrests for violations of State or Federal law.

CRIMINAL PENALTY

SEC. 302. (a) An officer or employee of any Federal agency who willfully keeps an information system without meeting the notice requirements of this Act set forth in section 201(c) shall be fined not more than $2,000 in each instance or imprisoned not more than two years, or both.

(b) Whoever, being an officer or employee of the Commission, shall disseminate any personal information about any individual obtained in the course of such officer or employee's duties in any manner or for any purpose not specifically authorized by law shall be fined not more than $10,000, or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 303. (a) Any individual who is denied access to information required to be disclosed under the provisions of this Act may bring a civil action in the appropriate district court of the United States for damages or other ap-

propriate relief against the Federal agency which denied access to such information.

(b) The Attorney General of the United States, or any aggrieved person, may bring an action in the appropriate United States district court against any person who is engaged or is about to engage in any acts or practices in violation of the provisions of this Act, to enjoin such acts or practices.

(c) The United States shall be liable for the actions or omissions of any officer or employee of the Government who violates the provisions of this Act, or any rule, regulation, or order issued thereunder in the same manner and to the same extent as a private individual under like circumstances to any person aggrieved thereby in an amount equal to the sum of—

(1) any actual and general damages sustained by any person but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(d) The United States consents to be sued under this section without limitation on the amount in controversy. A civil action against the United States under subsection (c)

of this section shall be the exclusive remedy for the wrongful action or omission of any officer or employee.

JURISDICTION OF DISTRICT COURTS

SEC. 304. (a) The district courts of the United States have jurisdiction to hear and determine civil actions brought under section 303 of this Act and may examine the information in camera to determine whether such information or any part thereof may be withheld under any of the exemptions in section 203 of this Act. The burden is on the Federal agency to sustain such action.

(b) In any action to obtain judicial review of a decision to exempt any personal information from any provision of this Act, the court may examine such information in camera to determine whether such information or any part thereof is properly classified with respect to national defense, foreign policy or law enforcement intelligence information or investigative information and may be exempted from any provision of this Act. The burden is on the Federal agency to sustain any claim that such information may be so exempted.

EFFECTIVE DATE

SEC. 305. This Act shall become effective one year after the date of enactment except that the provisions of title I of this Act shall become effective on the date of enactment.

AUTHORIZATION OF APPROPRIATIONS

SEC. 306. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.

MORATORIUM ON USE OF SOCIAL SECURITY NUMBERS

SEC. 307. (a) It shall be unlawful for—

(1) any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number, or

(2) any person to discriminate against any individual in the course of any business or commercial transaction or activity because of such individual's refusal to disclose his social security account number.

(b) The provisions of subsection (a) shall not apply with respect to—

(1) any disclosure which is required by Federal law, or

(2) any information system in existence and operating before January 1, 1975.

(c) Any Federal, State, or local government agency which requests an individual to disclose his social security account number, and any person who requests, in the course of any business or commercial transaction or activity, an individual to disclose his social security account number,

63-619 O - 76 - 25

shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

Passed the Senate November 21, 1974.

Attest:

Secretary.

93D CONGRESS
2D SESSION

H. R. 16373

IN THE SENATE OF THE UNITED STATES

NOVEMBER 22, 1974

Received; read twice, considered, amended, read the third time, and passed

[Insert the part printed in italic]

AN ACT

To amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, ~~That this Act may be cited as the "Privacy Act of 1974".~~

~~SEC. 2. (a) The Congress finds that—~~

~~(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;~~

~~(2) the increasing use of computers and sophisti-~~

cated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertain-

ing to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such informaton;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful, arbitrary, or capricious action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any collection or grouping of information about an individual that is maintained by an agency and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual; and

"(6) the term 'statistical research or reporting record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records

by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) for a routine use described under subsection (e) (2) (D) of this section;

"(3) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(4) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(5) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(6) to another agency or to an instrumentality of any governmental jurisdiction within or under the con-

trol of the United States for a law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(7) to a person who is actively engaged in saving the life of such individual, if upon such disclosure notification is transmitted to the last known address of such individual;

"(8) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee; or

"(9) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES. Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsection (b)(1) of this section or disclosures to the public from records which by law or regulation are open to public inspection or copying, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to an

other agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b) (6) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency within two years preceding the making of the correction of the record of the individual, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section or for which no accounting of the disclosure is required.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him to review

the record and have a copy made of all or any portion thereof in a form comprehensible to him;

"(2) permit the individual to request amendment of a record pertaining to him and either—

"(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(B) promptly inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

"(3) permit any individual who disagrees with the refusal of the agency to amend his record to request review of the refusal by the official named in accordance with paragraph (2) (B) of this subsection; and if, after the review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency;

"(4) in any disclosure, containing information

about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and, upon request, provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) which Federal statute or regulation, if any, requires disclosure of the information;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) other purposes for which the information may be used, as published pursuant to paragraph

~~(2) (D) of this subsection; and~~

~~"(D) the effects on him, if any, of not providing all or any part of the requested information;~~

~~"(2) subject to the provisions of paragraph (3) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—~~

~~"(A) the name and location of the system;~~

~~"(B) the categories of individuals on whom records are maintained in the system;~~

~~"(C) the categories of records maintained in the system;~~

~~"(D) each routine purpose for which the records contained in the system are used or intended to be used, including the categories of users of the records for each such purpose;~~

~~"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;~~

~~"(F) the title and business address of the agency official who is responsible for the system of records;~~

~~"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; and~~

~~"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content;~~

~~"(3) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;~~

~~"(4) maintain no record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained: *Provided, however*, That the provisions of this paragraph shall not be deemed to prohibit the maintenance of any record of activity which is pertinent to and within the scope of a duly authorized law enforcement activity; and~~

~~"(5) at least 30 days prior to publication of information under paragraph (2) (D) of this subsection published in the Federal Register notice of the use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.~~

~~"(f) AGENCY RULES.—In order to carry out the provi-~~

sions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means the head of

~~the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and~~

~~"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.~~

~~The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e) (2) of this section in a form available to the public at low cost.~~

~~"(g) (1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d) (1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of record, and consequently a determination is made which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.~~

~~"(2) (A) In any suit brought under the provisions of~~

~~subsection (g) (1) (A) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.~~

~~"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.~~

~~"(3) In any suit brought under the provisions of subsection (g) (1) (B) or (C) of this section in which the court determines that the agency acted in a manner which was willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—~~

~~"(A) actual damages sustained by the individual as a result of the refusal or failure; and~~

~~"(B) the costs of the action together with reasonable attorney fees as determined by the court.~~

~~"(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or~~

has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i) (1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or

~~agency not entitled to receive it, shall be fined not more than $5,000.~~

~~"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.~~

~~"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from any~~ part of this section except subsections (b) and (e) (2) (A) ~~through (F) and (i) if the system of records is—~~

~~"(1) maintained by the Central Intelligence Agency; or~~

~~"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement,~~

~~release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.~~

~~"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from subsections (c) (3), (d), (e) (1), (e) (2) (G) and (H), and (f) of this section if the system of records is—~~

~~"(1) subject to the provisions of section 552 (b) (1) of this title;~~

~~"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j) (2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal~~

the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

"(4) required by statute to be maintained and used solely as statistical research or reporting records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which

would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

"(l) (1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the

~~United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section.~~

~~"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsections (c) (4); (d) (2), (3), and (4); (e) (1), (2) (H) and (3); (f) (1); (g) (1) (B) and (C), and (3).~~

~~"(m) (1) MORATORIUM ON THE USE OF THE SOCIAL SECURITY ACCOUNT NUMBER.—No Federal agency, or any State or local government acting in compliance with any Federal law or federally assisted program, shall deny any individual any right, benefit, or privilege provided by law by reason of such individual's refusal to disclose his social security account number.~~

~~"(2) This subsection shall not apply—~~

~~"(A) with respect to any system of records in existence and operating prior to January 1, 1975; and~~

"(B) when disclosure of a social security account number is required by Federal law.

"(3) No Federal agency, or any State or local government acting in compliance with any Federal law or federally assisted program, shall use the social security account number for any purpose other than for verification of the identity of an individual unless such other purpose is specifically authorized by Federal law.

"(n) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.".

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings.".

~~SEC. 5. The amendments made by this Act shall become effective on the one hundred and eightieth day following the date of enactment of this Act.~~

TITLE I—PRIVACY PROTECTION COMMISSION

ESTABLISHMENT OF COMMISSION

SEC. 101. (a) There is established as an independent agency of the executive branch of the Government the Privacy Protection Commission.

(b)(1) The Commission shall be composed of five members who shall be appointed by the President, by and with the advice and consent of the Senate, from among members of the public at large who, by reason of their knowledge and expertise in any of the following areas: civil rights and liberties, law, social sciences, and computer technology, business, and State and local government, are well qualified for service on the Commission and who are not otherwise officers or employees of the United States. Not more than three of the members of the Commission shall be adherents of the same political party.

(2) One of the Commissioners shall be appointed Chairman by the President.

(3) A Commissioner appointed as Chairman shall serve as Chairman until the expiration of his term as a Commissioner of the Commission (except that he may continue to serve as Chairman for so long as he remains a Commissioner and his successor as Chairman has not taken office). An individual may be appointed as a Commissioner at the same time he is appointed Chairman.

(c) The Chairman shall preside at all meetings of the Commission and a quorum for the transaction of business shall consist of at least three members present (but the Chairman may designate an Acting Chairman who may preside in the absence of the Chairman). Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information relating to the performance of his duties or responsibilities, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or Acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, persons, or the public, and, on behalf of the Commission, shall see to the faithful execution of the policies and

decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

(d) Each Commissioner shall be compensated at the rate provided for under section 5314 of title 5 of the United States Code, relating to level IV of the Executive Schedule.

(e) Commissioners shall serve for terms of three years. No Commissioner may serve more than two terms. Vacancies in the membership of the Commission shall be filled in the same manner in which the original appointment was made.

(f) Vacancies in the membership of the Commission, as long as there are three Commissioners in office, shall not impair the power of the Commission to execute the functions and powers of the Commission.

(g) The members of the Commission shall not engage in any other employment during their tenure as members of the Commission.

(h)(1) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress.

(2) Whenever the Commission submits any legislative

recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress.

PERSONNEL OF THE COMMISSION

SEC. 102. (a)(1) The Commission shall appoint an Executive Director who shall perform such duties as the Commission may determine. Such appointment may be made without regard to the provisions of title 5, United States Code.

(2) The Executive Director shall be compensated at a rate not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of title 5, United States Code.

(b) The Commission is authorized to appoint and fix the compensation of such officers and employees, and prescribe their functions and duties, as may be necessary to carry out the provisions of this Act.

(c) The Commission may obtain the services of experts

and consultants in accordance with the provisions of section 3109 of title 5, United States Code.

FUNCTIONS OF THE COMMISSION

SEC. 103. (a) The Commission shall—

(1) publish annually a United States Directory of Information Systems containing the information specified to provide notice under section 201(c)(3) of this Act for each information system subject to the provisions of this Act and a listing of all statutes which require the collection of such information by a Federal agency;

(2) investigate, determine, and report any violation of any provision of this Act (or any regulation adopted pursuant thereto) to the President, the Attorney General, the Congress, and the General Services Administration where the duties of that agency are involved, and to the Comptroller General when it deems appropriate; and

(3) develop model guidelines for the implementation of this Act and assist Federal agencies in preparing regulations and meeting technical and administrative requirements of this Act.

(b) Upon receipt of any report required of a Federal agency describing (1) any proposed information system or data bank, or (2) any significant expansion of an existing information system or data bank, integration of files, programs for records linkage within or among agencies, or cen-

tralization of resources and facilities for data processing, the Commission shall—

(A) review such report to determine (i) the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the confidentiality of information relating to such individuals, and (ii) its effect on the preservation of the constitutional principles of federalism and separation of powers; and

(B) submit findings and make recommendations to the President, Congress, and the General Services Administration concerning the need for legislative authorization and administrative action relative to any such proposed activity in order to meet the purposes and requirements of this Act.

(c) After receipt of any report required under subsection (b), if the Commission determines and reports to the Congress that a proposal to establish or modify a data bank or information system does not comply with the standards established by or pursuant to this Act, the Federal agency submitting such report shall not proceed to establish or modify any such data bank or information system for a period of sixty days from the date of receipt of notice from the Commission that such data bank or system does not comply with such standards.

(d) In addition to its other functions the Commission shall—

(1) to the fullest extent practicable, consult with the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out the provisions of this Act and in conducting the study required by section 106 of this Act;

(2) perform or cause to be performed such research activities as may be necessary to implement title II of this Act, and to assist Federal agencies in complying with the requirements of such title;

(3) determine what specific categories of information should be prohibited by statute from collection by Federal agencies on the basis that the collection of such information would violate an individual's right of privacy; and

(4) prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation.

CONFIDENTIALITY OF INFORMATION

SEC. 104. (a) Each department, agency, and instrumentality of the executive branch of the Government, including each independent agency, shall furnish to the Commission, upon request made by the Chairman, such data, reports, and other information as the Commission deems necessary to carry out its functions under this Act.

(b) In carrying out its functions and exercising its powers under this Act, the Commission may accept from any Federal agency or other person any identifiable personal data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall provide appropriate safeguards to insure that the confidentiality of such information is maintained and that upon completion of the purpose for which such information is required it is destroyed or returned to the agency or person from which it is obtained, as appropriate.

POWERS OF THE COMMISSION

SEC. 105. (a)(1) The Commission may, in carrying out its functions under this Act, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures

as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Commission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2) In case of disobedience to a subpena issued under paragraph (1) of this subsection, the Commission may invoke the aid of any district court of the United States in requiring compliance with such subpena. Any district court of the United States within the jurisdiction where such person is found or transacts business may, in case of contumacy or refusal to obey a subpena issued by the Commission, issue an order requiring such person to appear and testify, to produce such books, records, papers, correspondence, and documents, and any failure to obey the order of the court shall be punished by the court as a contempt thereof.

(3) Appearances by the Commission under this Act shall be in its own name. The Commission shall be represented by attorneys designated by it.

(4) Section 6001(1) of title 18, United States Code, is amended by inserting immediately after "Securities and

Exchange Commission," the following: "the Privacy Protection Commission,".

(b) The Commission may delegate any of its functions to such officers and employees of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(c) In order to carry out the provisions of this Act, the Commission is authorized—

(1) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(2) to adopt, amend, and repeal interpretative rules for the implementation of the rights, standards, and safeguards provided under this Act;

(3) to enter into contracts or other arrangements or modifications thereof, with any government, any agency or department of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(4) to make advance, progress, and other payments which the Commission deems necessary under this Act

63-619 O - 76 - 27

without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529);

(5) receive complaints of violations of this Act and regulations adopted pursuant thereto; and

(6) to take such other action as may be necessary to carry out the provisions of this Act.

COMMISSION STUDY OF OTHER GOVERNMENTAL AND PRIVATE ORGANIZATIONS

SEC. 106. (a)(1) The Commission shall make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information, and to determine the extent to which those standards and procedures achieve the purposes of this Act.

(2) The Commission periodically shall report its findings to the President and the Congress and shall complete the study required by this section not later than three years from the date this Act becomes effective.

(3) The Commission shall recommend to the President and the Congress the extent, if any, to which the requirements and principles of this Act should be applied to the information practices of those organizations by legislation, administrative action, or by voluntary adoption of such requirements and

principles. In addition, it shall submit such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

(b)(1) In the course of such study and in its reports, the Commission shall examine and analyze—

(A) interstate transfer of information about individuals which is being undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the im-

plied or explicitly recognized confidentiality of such information.

(2) The Commission shall include in its examination information activities in the following areas: medical, insurance, education, employment and personnel, credit, banking and financial institutions, credit bureaus, the commercial reporting industry, cable television, and other telecommunications media, travel, hotel, and entertainment reservations, and electronic check processing. The Commission may study such other information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

(3) In conducting the study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) conduct a thorough examination of standards and criteria governing programs, policies, and practices

relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information;

(D) to the maximum extent practicable, collect and utilize findings, reports, and recommendations of major governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission; and

(E) receive and review complaints with respect to any matter under study by the Commission which may be submitted by any person.

REPORTS

SEC. 107. The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this Act.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, INTELLIGENCE, STATISTICAL-REPORTING, AND RESEARCH PURPOSES

SEC. 201. (a) Each Federal agency shall—

(1) collect, solicit, and maintain only such personal information as is relevant and necessary to accomplish a statutory purpose of the agency;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs; and

(3) inform any individual requested to disclose personal information whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, will result from nondisclosure, and what rules of confidentiality will govern the information.

(b) Each Federal agency that maintains an information system or file shall, with respect to each such system or file—

(1) insure that personal information maintained in the system or file is accurate, complete, timely, and relevant to the purpose for which it is collected or maintained by the agency at the time any access is granted to the file, material is added to or taken from the file, or at any time it is used to make a determination affecting the subject of the file;

(2) refrain from disclosing any such personal information within the agency other than to officers or employees who have a need for such personal information in the performance of their duties for the agency;

(3) maintain a list of all categories of persons authorized to have regular access to personal information in the system or file;

(4) maintain an accurate accounting of the date, nature, and purpose of all other access granted to the system or file, and all other disclosures of personal information made to any person outside the agency, or to another agency, including the name and address of the person or other agency to whom disclosure was made or access was granted, except as provided by section 202 (b) of this Act;

(5) establish rules of conduct and notify and instruct each person involved in the design, development, operation, or maintenance of the system or file, or the collection, use, maintenance, or dissemination of information about an individual, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance;

(6) establish appropriate administrative, technical and physical safeguards to insure the security of the information system and confidentiality of personal information and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience,

or unfairness to any individual on whom personal information is maintained; and

(7) establish no program for the purpose of collecting or maintaining information describing how individuals exercise rights guaranteed by the first amendment unless the head of the agency specifically determines that such information is relevant and necessary to carry out a statutory purpose of the agency.

(c) Any Federal agency that maintains an information system or file shall—

(1) make available for distribution upon the request of any person a statement of the existence and character of each such system or file;

(2) on the date on which this Act becomes effective and annually thereafter, notify the Commission and give public notice of the existence and character of each existing system or file simultaneously, and cause such notice to be published in the Federal Register; and

(3) include in such notices at least the following information:

(A) name and location of the system or file;

(B) nature and purposes of the system or file;

(C) categories of individuals on whom personal information is maintained and categories of personal

information generally maintained in the system or file, including the nature of the information and the approximate number of individuals on whom information is maintained;

(D) the confidentiality requirements and the extent to which access controls apply to such information;

(E) categories of sources of such personal information;

(F) the Federal agency's policies and practices regarding implementation of sections 201 and 202 of this Act, information storage, duration of retention of information, and elimination of such information from the system or file;

(G) uses made by the agency of the personal information contained in the system or file;

(H) identity of other agencies and categories of persons to whom disclosures of personal information are made, or to whom access to the system or file may be granted, together with the purposes therefor and the administrative constraints, if any, on such disclosures and access, including any such constraints on redisclosure;

(I) procedures whereby an individual can (i) be informed if the system or file contains personal

information pertaining to himself or herself, (ii) gain access to such information, and (iii) contest the accuracy, completeness, timeliness, relevance, and necessity for retention of the personal information; and

(J) name, title, official address, and telephone number of the officer immediately responsible for the system or file.

(d)(1) Each Federal agency that maintains an information system or file shall assure to an individual upon request the following rights:

(A) to be informed of the existence of any personal information pertaining to that individual;

(B) to have full access to and right to inspect the personal information in a form comprehensible to the individual;

(C) to know the names of all recipients of information about such individual including the recipient organization and its relationship to the system or file, and the purpose and date when distributed, unless such information is not required to be maintained pursuant to this Act;

(D) to know the sources of personal information (i) unless the confidentiality of any such source is required by statute, then the right to know the nature of such

source; or (ii) unless investigative material used to determine the suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, is compiled by a Federal agency in pursuit of an authorized investigative responsibility, and in the course of compiling such materials, information prejudicial to the subject of the investigation is revealed through a source who furnishes such information to the Government under the express provision that the identity of the source will be held in confidence, and where the disclosure of such information would identify and be prejudicial to the rights of the confidential source, then the right to know the nature of such information and to examine that information if it is found to be material or relevant to an administrative or judicial proceeding by a Federal judge or Federal administrative officer: Provided, That investigative material shall not be made available to promotion boards which are empowered to promote or advance individuals in Federal employment, except when the appointment would be from a noncritical to a critical security position;

(E) to be accompanied by a person chosen by the individual inspecting the information, except that an agency or other person may require the individual to

furnish a written statement authorizing discussion of that individual's file in the person's presence;

(F) to receive such required disclosures and at reasonable standard charges for document duplication, in person or by mail, if upon written request, with proper identification; and

(G) to be completely informed about the uses and disclosures made of any such information contained in any such system or file except those uses and disclosures made pursuant to law or regulation permitting public inspection or copying.

(2) Upon receiving notice that an individual wishes to challenge, correct, or explain any personal information about him in a system or file, such Federal agency shall comply promptly with the following minimum requirements:

(A) investigate and record the current status of the personal information;

(B) correct or eliminate any information that is found to be incomplete, inaccurate, not relevant to a statutory purpose of the agency, not timely or necessary to be retained, or which can no longer be verified;

(C) accept and include in the record of such information, if the investigation does not resolve the dispute, any statement of reasonable length provided by the

individual setting forth his position on the disputed information;

(D) in any subsequent dissemination or use of the disputed information, clearly report the challenge and supply any supplemental statement filed by the individual;

(E) at the request of such individual, following any correction or elimination of challenged information, inform past recipients of its elimination or correction; and

(F) not later than sixty days after receipt of notice from an individual making a request concerning personal information, make a determination with respect to such request and notify the individual of the determination and of the individual's right to a hearing before an official of the agency which shall if requested by the individual, be conducted as follows:

(i) such hearing shall be conducted in an expeditious manner to resolve the dispute promptly and shall be held within thirty days of the request and, unless the individual requests a formal hearing, shall be conducted on an informal basis, except that the individual may appear with counsel, present evidence, and examine and cross-examine witnesses;

(ii) any record found after such a hearing to be incomplete, inaccurate, not relevant, not timely,

nor necessary to be retained, or which can no longer be verified, shall within thirty days of the date of such findings be appropriately modified or purged; and

(iii) the action or inaction of any agency on a request to review and challenge personal data in its possession as provided by this section shall be reviewable de novo by the appropriate United States district court.

An agency may, for good cause, extend the time for making a determination under this subparagraph. The individual affected by such an extension shall be given notice of the extension and the reason therefore.

(e) When a Federal agency provides by a contract, grant, or agreement for, and the specific creation or substantial alteration, or the operation by or on behalf of the agency of an information system or file and the primary purpose of the grant, contract, or agreement is the creation, substantial alteration, or the operation by or on behalf of the agency of such an information system or file, the agency shall, consistent with its authority, cause the requirements of subsections (a), (b), (c), and (d) to be applied to such system or file. In cases when contractors and grantees or parties to an agreement are public agencies of States or the District of Columbia or public agencies of political subdivi-

sions of States, the requirements of subsections (a), (b), (c), and (d) shall be deemed to have been met if the Federal agency determines that the State or the District of Columbia or public agencies of political subdivisions of the State have adopted legislation or regulations which impose similar requirements.

(f)(1) Any Federal agency maintaining or proposing to establish a personal information system or file shall prepare and submit a report to the Commission, the General Services Administration, and to the Congress on proposed data banks and information systems or files, the proposed significant expansion of existing data banks and information systems or files, integration of files, programs for records linkage within or among agencies, or centralization of resources and facilities for data processing, which report shall include—

(A) the effects of such proposals on the rights, benefits, and privileges of the individuals on whom personal information is maintained;

(B) a statement of the software and hardware features which would be required to protect security of the system or file and confidentiality of information;

(C) the steps taken by the agency to acquire such features in their systems, including description of con-

sultations with representatives of the National Bureau of Standards; and

(D) a description of changes in existing interagency or intergovernmental relationships in matters involving the collection, processing, sharing, exchange, and dissemination of personal information.

(2) The Federal agency shall not proceed to implement such proposal for a period of sixty days from date of receipt of notice from the Commission that the proposal does not comply with the standards established under or pursuant to this Act.

(g) Each Federal agency covered by this Act which maintains an information system or file shall make reasonable efforts to serve advance notice on an individual before any personal information on such individual is made available to any person under compulsory legal process.

(h) No person may condition the granting or withholding of any right, privilege, or benefit, or make as a condition of employment the securing by any individual of any information which such individual may obtain through the exercise of any right secured under the provisions of this section.

DISCLOSURE OF INFORMATION

SEC. 202. (a) No Federal agency shall disseminate personal information unless—

(1) it has made written request to the individual who is the subject of the information and obtained his written consent;

(2) the recipient of the personal information has adopted rules in conformity with this Act for maintaining the security of its information system and files and the confidentiality of personal information contained therein; and

(3) the information is to be used only for the purposes set forth by the sender pursuant to the requirements for notice under this Act.

(b) Section 202(a)(1) shall not apply when disclosure would be—

(1) to those officers and employees of that agency who have a need for such information in ordinary course of the performance of their duties;

(2) to the Bureau of the Census for purposes of planning or carrying out a census or survey pursuant to the provisions of title 13, United States Code: Provided, that such personal information is transferred or disseminated in a form not individually identifiable.

(3) where the agency determines that the recipient of such information has provided advance adequate written assurance that the information will be used solely as a statistical reporting or research record, and is to be

63-619 O - 76 - 28

transferred in a form that is not individually identifiable; or

(4) pursuant to a showing of compelling circumstances affecting health or safety of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.

(c) Section 201(b)(4) and paragraphs (1), (2), and (3) of subsection (a) of this section shall not apply when disclosure would be to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office. Nothing in this Act shall impair access by the Comptroller General, or any of his authorized representatives, to records maintained by an agency, including records of personal information, in the course of performance of such duties.

(d)(1) Nothing in this section shall be construed to limit the efforts of the Government pursuant to the provisions of chapter 35, title 44 of the United States Code (commonly known as the Federal Reports Act) or any other statute, to reduce the burden on citizens of collecting information by means of combining or eliminating unnecessary reports, questionnaires, or requests for information.

(2) Nothing in this section shall be construed to affect restrictions on the exchange of information between agencies

as required by chapter 35, title 44 of the United States Code (commonly known as the Federal Reports Act).

(e) Subsection (a)(1) of this section shall not apply when disclosure would be to another agency or to an instrumentality of any governmental jurisdiction for a law enforcement activity if such activity is authorized by statute and if the head of such agency or instrumentality has made a written request to or has an agreement with the agency which maintains the system or file specifying the particular portion of the information desired and the law enforcement activity for which the information is sought.

EXEMPTIONS

SEC. 203. (a) The provisions of section 201(c)(3)(E), (d), and section 202, shall not apply to any personal information contained in any information system or file if the head of the Federal agency determines, in accordance with the provisions of this section, that the application of the provisions of any such sections would seriously damage national defense or foreign policy or where the application of any such provisions would seriously damage or impede the purpose for which the information is maintained.

(b) The provisions of section 201(d) and section 202 shall not apply to law enforcement intelligence information or investigative information if the head of the Federal agency determines, in accordance with the provisions of any of such

sections would seriously damage or impede the purpose for which the information is maintained: Provided, That investigatory records shall be exempted only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) disclose the identity of a confidential source, and in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source, (E) disclose confidential investigative techniques and procedures which are not otherwise generally known outside the agency, or (F) endangers the life or physical safety of law enforcement personnel: Provided, That investigative information may not be exempted under this section where such information has been maintained for a period longer than is necessary to commence criminal prosecution. Nothing in this Act shall prohibit the disclosure of such investigative information to a party in litigation where required by statute or court rule.

(c)(1) A determination to exempt any such system, file, or information may be made by the head of any such agency in accordance with the requirements of notice, publication, and hearing contained in sections 553 (b), (c), and (e), 556, and 557 of title 5, United States Code. In giving notice

of an intent to exempt any such system, file, or information, the head of such agency shall specify the nature and purpose of the system, file, or information to be exempted.

(2) Whenever any Federal agency undertakes to exempt any information system, file, or information from the provisions of this Act, the head of such Federal agency shall promptly notify the Commission of its intent and afford the Commission opportunity to comment.

(3) The exception contained in section 553(d) of title 5, United States Code (allowing less than thirty days' notice), shall not apply in any determination made or any proceeding conducted under this section.

ARCHIVAL RECORDS

SEC. 204. (a) Federal agency records which are accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44, United States Code, shall, for the purposes of this section, be considered to be maintained by the agency which deposited the records and shall be subject to the provisions of this Act. The Administrator of General Services shall not disclose such records, or any information therein, except to the agency which maintains the records or pursuant to rules established by that agency.

(b) Federal agency records pertaining to identifiable individuals which were transferred to the National Archives

of the United States as records which have sufficient historical or other value to warrant their continued preservation by the United States Government shall for the purposes of this Act, be considered to be maintained by the National Archives and shall not be subject to the provisions of this Act except section 201(b) (5) and (6).

(c) The National Archives shall, on the date on which this Act becomes effective and annually thereafter, notify the Commission and give public notice of the existence and character of the information systems and files which it maintains, and cause such notice to be published in the Federal Register. Such notice shall include at least the information specified under section 201(c)(3) (A), (B), (D), (E), (F), (G), (I), and (J).

EXCEPTIONS

SEC. 205. (a) No officer or employee of the executive branch of the Government shall rely on any exemption in subchapter II of chapter 5 of title 5 of the United States Code commonly known as the Freedom of Information Act) to withhold information relating to an individual otherwise accessible to an individual under this Act.

(b) Nothing in this Act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder.

(c) The provisions of section 201(d)(1) of this Act shall not apply to records collected or furnished and used by the Bureau of the Census solely for statistical purposes or as authorized by section 8 of title 13 of the United States Code: Provided, That such personal information is transferred or disseminated in a form not individually identifiable.

(d) The provisions of this Act shall not require the disclosure of testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service if the disclosure of such material would compromise the objectivity or fairness of the testing or examination process.

(e) The provisions of this Act, with the exception of sections 201(a)(2), 201(b) (2), (3), (4), (5), (6), and (7), 201(c)(2), 201(c)(3) (A), (B), (D), and (F), and 202 (a) (2) and (3) shall not apply to foreign intelligence information systems or to systems of personal information involving intelligence sources and methods designed for protection from unauthorized disclosure pursuant to 50 U.S.C. 403.

MAILING LISTS

SEC. 206. (a) An individual's name and address may not be sold or rented by a Federal agency unless such action is specifically authorized by law. This provision shall not be

construed to require the confidentiality of names and addresses otherwise permitted to be made public.

(b) Upon written request of any individual, any person engaged in interstate commerce who maintains a mailing list shall remove the individual's name and address from such list.

REGULATIONS

SEC. 207. Each Federal agency subject to the provisions of this Act shall, not later than six months after the date on which this Act becomes effective, promulgate regulations to implement the standards, safeguards, and access requirements of this title and such other regulations as may be necessary to implement the requirements of this Act.

TITLE III—MISCELLANEOUS

DEFINITIONS

SEC. 301. As used in this Act—

(1) the term "Commission" means the Privacy Protection Commission;

(2) the term "personal information" means any information that identifies or describes any characteristic of an individual, including, but not limited to, his education, financial transactions, medical history, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice

prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

(3) the term "individual" means a citizen of the United States or an alien lawfully admitted through permanent residence;

(4) the term "information system" means the total components and operations, whether automated or manual, by which personal information, including name or identifier, is collected, stored, processed, handled, or disseminated by an agency;

(5) the term "file" means a record or series of records containing personal information about individuals which may be maintained within an information system;

(6) the term "data bank" means a file or series of files pertaining to individuals;

(7) the term "Federal agency" means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof;

(8) the term "investigative information" means information associated with an identifiable individual compiled by—

(A) an agency in the course of conducting a

criminal investigation of a specific criminal act where such investigation is pursuant to a statutory function of the agency. Such information may pertain to that criminal act and be derived from reports of informants and investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically and expressly required by State or Federal statute to be made public; or

(B) by an agency with regulatory jurisdiction which is not a law enforcement agency in the course of conducting an investigation of specific activity which falls within the agency's regulatory jurisdiction. For the purposes of this paragraph, an "agency with regulatory jurisdiction" is an agency which is empowered to enforce any Federal statute or regulation, the violation of which subjects the violator to criminal or civil penalties;

(9) the term "law enforcement intelligence information" means information associated with an identifiable individual compiled by a law enforcement agency in the course of conducting an investigation of an individual in anticipation that he may commit a

specific criminal act, including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically by incident and expressly required by State or Federal statute to be made public;

(10) the term "criminal history information" means information on an individual consisting of notations of arrests, detentions, indictments, informations, or other formal criminal charges and any disposition arising from those arrests, detentions, indictments, informations, or charges. The term shall not include an original book of entry or police blotter maintained by a law enforcement agency at the place of an original arrest or place of detention, indexed chronologically and required to be made public, nor shall it include court records of public criminal proceedings indexed chronologically; and

(11) the term "law enforcement agency" means an agency whose employees or agents are empowered by State or Federal law to make arrests for violations of State or Federal law.

CRIMINAL PENALTY

SEC. 302. (a) Any officer or employee of any Federal agency who willfully keeps an information system without meeting the notice requirements of this Act set forth in section 201(c) shall be fined not more than $2,000 in each instance or imprisoned not more than two years, or both.

(b) Whoever, being an officer or employee of the Commission, shall disseminate any personal information about any individual obtained in the course of such officer or employee's duties in any manner or for any purpose not specifically authorized by law shall be fined not more than $10,000, or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 303. (a) Any individual who is denied access to information required to be disclosed under the provisions of this Act may bring a civil action in the appropriate district court of the United States for damages or other appropriate relief against the Federal agency which denied access to such information.

(b) The Attorney General of the United States, or any aggrieved person, may bring an action in the appropriate United States district court against any person who is engaged or is about to engage in any acts or practices in

violation of the provisions of this Act, to enjoin such acts or practices.

(c) The United States shall be liable for the actions or omissions of any officer or employee of the Government who violates the provisions of this Act, or any rule, regulation, or order issued thereunder in the same manner and to the same extent as a private individual under like circumstances to any person aggrieved thereby in an amount equal to the sum of—

(1) any actual and general damages sustained by any person but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(d) The United States consents to be sued under this section without limitation on the amount in controversy. A civil action against the United States under subsection (c) of this section shall be the exclusive remedy for the wrongful action or omission of any officer or employee.

JURISDICTION OF DISTRICT COURTS

SEC. 304. (a) The district courts of the United States have jurisdiction to hear and determine civil actions brought

under section 303 of this Act and may examine the information in camera to determine whether such information or any part thereof may be withheld under any of the exemptions in section 203 of this Act. The burden is on the Federal agency to sustain such action.

(b) In any action to obtain judicial review of a decision to exempt any personal information from any provision of this Act, the court may examine such information in camera to determine whether such information or any part thereof is properly classified with respect to national defense, foreign policy or law enforcement intelligence information or investigative information and may be exempted from any provision of this Act. The burden is on the Federal agency to sustain any claim that such information may be so exempted.

EFFECTIVE DATE

SEC. 305. This Act shall become effective one year after the date of enactment except that the provisions of title I of this Act shall become effective on the date of enactment.

AUTHORIZATION OF APPROPRIATIONS

SEC. 306. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.

MORATORIUM ON USE OF SOCIAL SECURITY NUMBERS

SEC. 307. (a) It shall be unlawful for—

(1) any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number, or

(2) any person to discriminate against any individual in the course of any business or commercial transaction or activity because of such individual's refusal to disclose his social security account number.

(b) The provisions of subsection (a) shall not apply with respect to—

(1) any disclosure which is required by Federal law, or

(2) any information system in existence and operating before January 1, 1975.

(c) Any Federal, State, or local government agency which requests an individual to disclose his social security account number, and any person who requests, in the course of any business or commercial transaction or activity, an individual to disclose his social security account number, shall

inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

Passed the House of Representatives November 21, 1974.

Attest: W. PAT JENNINGS,
Clerk.

Passed the Senate November 22, 1974.

Attest: FRANCIS R. VALEO,
Secretary.

In the House of Representatives, U. S.,

December 11, 1974.

Resolved, That the bill from the Senate (S. 3418) entitled "An Act to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes", do pass with the following

AMENDMENTS:

Strike out all after the enacting clause, and insert:

That this Act may be cited as the "Privacy Act of 1974".

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure

63-619 O - 76 - 29

employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to

have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful, arbitrary, or capricious action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the

United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any collection or grouping of information about an individual that is maintained by an agency and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual; and

"(6) the term 'statisical research or reporting record' means a record in a system of records maintained for statisical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the

prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) for a routine use described under subsection (e)(2)(D) of this section;

"(3) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(4) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(5) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(6) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity

if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(7) to a person who is actively engaged in saving the life of such individual, if upon such disclosure notification is transmitted to the last known address of such individual;

"(8) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee; or

"(9) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsection (b)(1) of this section or disclosures to the public from records which by law or regulation are open to public inspection or copying, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to an-

other agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(6) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency within two years preceding the making of the correction of the record of the individual, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section or for which no accounting of the disclosure is required.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him

which is contained in the system, permit him to review the record and have a copy made of all or any portion thereof in a form comprehensible to him;

"(2) permit the individual to request amendment of a record pertaining to him and either—

"(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(B) promptly inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

"(3) permit any individual who disagrees with the refusal of the agency to amend his record to request review of the refusal by the official named in accordance with paragraph (2)(B) of this subsection; and if, after the review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency;

"(4) in any disclosure, containing information

about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and, upon request, provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) which Federal statute or regulation, if any, requires disclosure of the information;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) other purposes for which the information

may be used, as published pursuant to paragraph (2)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

"(2) subject to the provisions of paragraph (5) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine purpose for which the records contained in the system are used or intended to be used, including the categories of users of the records for each such purpose;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; and

"(II) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content;

"(3) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(4) maintain no record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained: Provided, however, That the provisions of this paragraph shall not be deemed to prohibit the maintenance of any record of activity which is pertinent to and within the scope of a duly authorized law enforcement activity; and

"(5) at least 30 days prior to publication of information under paragraph (2)(D) of this subsection published in the Federal Register notice of the use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

"(f) AGENCY RULES.—In order to carry out the provi-

sions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means the head of

the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(2) of this section in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d)(1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of records and consequently a determination is made which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

"(2)(A) In any suit brought under the provisions of

subsection (g)(1)(A) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(3) In any suit brought under the provisions of subsection (g)(1) (B) or (C) of this section in which the court determines that the agency acted in a manner which was willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—

"(A) actual damages sustained by the individual as a result of the refusal or failure; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or

has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be bought at any time within two years after discovery by the individual of the misrepresentation.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or

agency not entitled to receive it, shall be fined not more than $5,000.

"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from any part of this section except subsections (b) and (e)(2)(A) through (F) and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement,

release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(2) (G) and (H), and (f) of this section if the system of records is—

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the

63-6[illegible] O - 76 - 30

Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

"(4) required by statute to be maintained and used solely as statistical research or reporting records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

"(l)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered

to be maintained by the National Archives and shall not be subject to the provisions of this section.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsections (c)(4); (d) (2), (3), and (4); (e) (1), (2)(H) and (3); (f)(4); (g)(1) (B) and (C), and (3).

"(m)(1) MORATORIUM ON THE USE OF THE SOCIAL SECURITY ACCOUNT NUMBER.—No Federal agency, or any State or local government acting in compliance with any Federal law or federally assisted program, shall deny any individual any right, benefit, or privilege provided by law by reason of such individual's refusal to disclose his social security account number.

"(2) This subsection shall not apply—

"(A) with respect to any system of records in existence and operating prior to January 1, 1975; and

"(B) when disclosure of a social security account number is required by Federal law.

"(3) No Federal agency, or any State or local govern-

ment acting in compliance with any Federal law or federally assisted program, shall use the social security account number for any purpose other than for verification of the identity of an individual unless such other purpose is specifically authorized by Federal law.

"(n) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.".

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings.".

SEC. 5. The amendments made by this Act shall become effective on the one hundred and eightieth day following the date of enactment of this Act.

Amend the title so as to read: "An Act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies."

Attest:

Clerk.

In the Senate of the United States,

December 17, 1974.

Resolved, That the Senate agree to the amendments of the House of Representatives to the bill (S. 3418) entitled "An Act to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes", with the following

SENATE AMENDMENTS TO HOUSE AMENDMENTS:

In lieu of the matter proposed to be inserted by the House engrossed amendment to the text of the bill, insert:

That this Act may be cited as the "Privacy Act of 1974".

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to

have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. **Records maintained on individuals**

"*(a) DEFINITIONS.—For purposes of this section—*

"*(1) the term 'agency' means agency as defined in section 552(e) of this title;*

"*(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;*

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

"(6) the term 'statistical record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13; and

"(7) the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall

disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) required under section 552 of this title;

"(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Adminis-

trator of General Services or his designee to determine whether the record has such value;

"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

"(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

"(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

"(11) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been discolsed to the person or agency if an accounting of the disclosure was made.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

"(2) permit the individual to request amendment of a record pertaining to him and—

"(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

"(B) promptly, either—

"(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures

established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

"(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after the review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide

copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

"(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

"(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) the authority (whether granted by stat-

ute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

"(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

63-619 O - 76 - 31

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

"(I) the categories of sources of records in the system;

"(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(6) prior to disseminating any record about an individual to any person other than an agency, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant;

"(7) maintain no record describing how any indi-

vidual exercises rights guaranteed by the first amendment unless expressly authorized by statute or by the individual about who the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

"(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

"(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

"(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarassment, inconvenience, or unfairness to any individual on whom information is maintained; and

"(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection,

publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

"(f) AGENCY RULES.— In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency—

"(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection:

"(B) refuses to comply with an individual request under subsection (d)(1) of this section;

"(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any

determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on such record, and consequently a determination is made which is adverse to the individual; or

"(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

"(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine

the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(4) In any suit brought under the provisions of subsection (g)(1) (C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

"(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without

regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be bought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) CRIMINAL PENALTIES.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully

discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

"(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

"(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c), (1), (2), and (4), (e)(4)(A) through (F) (e) (6), (7), (9), (10), and (11), and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws including police efforts to prevent, control, or reduce crime

or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title the reasons why the system of records is to be exempted from a provision of this section.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of this section if the system of records is—

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

"(4) required by statute to be maintained and used solely as statistical records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but

only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

"(l)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or

other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4) (A) through (G) and (e)(9) of this section.

"(m) GOVERNMENT CONTRACTORS.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

"(n) MAILING LISTS.—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

"(o) REPORT ON NEW SYSTEMS.—Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the

privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

"(p) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

"(q) EFFECT OF OTHER LAWS.—No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.".

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings.".

SEC. 5. (a)(1) There is established a Privacy Protection Study Commission (hereinafter referred to as the "Commission") which shall be composed of seven members as follows:

(A) three appointed by the President of the United States,

(B) two appointed by the President of the Senate, and

(C) two appointed by the Speaker of the House of Representatives.

Members of the Commission shall be chosen from among persons who, by reason of their knowledge and expertise in any of the following areas—civil rights and liberties, law, social sciences, computer technology, business, records management, and State and local governments—are well qualified for service on the Commission.

(2) The members of the Commission shall elect a Chairman from among themselves.

(3) Any vacancy in the membership of the Commission, as long as there are four members in office, shall not impair the power of the Commission but shall be filled in the same manner in which the original appointment was made.

(4) A quorum of the Commission shall consist of a majority of the members, except that the Commission may establish a lower number as a quorum for the purpose of

taking testimony. The Commission is authorized to establish such committees and delegate such authority to them as may be necessary to carry out its functions. Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information necessary to the performance of their functions, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or a member designated by the Chairman to be acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, other persons, and the public, and, on behalf of the Commission, shall see to the faithful execution of the administrative policies and decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

(5)(A) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress.

(B) Whenever the Commission submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No

63-619 O - 76 - 32

officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress.

(b) The Commission shall—

(1) make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information; and

(2) recommend to the President and the Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

(c)(1) In the course of conducting the study required under subsection (b)(1) of this section, and in its reports

thereon, the Commission may research, examine, and analyze—

(A) interstate transfer of information about individuals that is undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the implied or explicitly recognized confidentiality of such information.

(2)(A) The Commission may include in its examination personal information activities in the following areas:

medical; insurance; education; employment and personnel; credit, banking and financial institutions; credit bureaus; the commercial reporting industry; cable television and other telecommunications media; travel, hotel, and entertainment reservations; and electronic check processing.

(B) The Commission shall include in its examination a study of—

(i) whether a person engaged in interstate commerce who maintains a mailing list should be required to remove an individual's name and address from such list upon request of that individual;

(ii) whether the Internal Revenue Service should be prohibited from transfering individually indentifiable data to other agencies and to agencies of State governments;

(iii) whether the Federal Government should be liable for general damages incurred by an individual as the result of a willful or intentional violation of the provisions of sections 552a(g)(1) (C) or (D) of title 5, United States Code; and

(iv) whether and how the standards for security and confidentiality of records required under section 552a (e)(10) of such title should be applied when a record is disclosed to a person other than an agency.

(C) The Commission may study such other personal information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

(3) In conducting such study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) examine the standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information; and

(D) to the maximum extent practicable, collect and utilize findings, reports, studies, hearing transcripts, and recommendations of governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission.

(d) In addition to its other functions the Commission may—

(1) request assistance of the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out its functions under this Act;

(2) upon request, assist Federal agencies in complying with the requirements of section 552a of title 5, United States Code;

(3) determine what specific categories of information, the collection of which would violate an individual's right of privacy, should be prohibited by statute from collection by Federal agencies; and

(4) upon request, prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation of implementation of such legislation.

(e)(1) The Commission may, in carrying out its functions under this section, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers,

correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Commission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2)(A) Each department, agency, and instrumentality of the executive branch of the Government is authorized to furnish to the Commission, upon request made by the Chairman, such information, data, reports, and such other assistance as the Commission deems necessary to carry out its functions under this section. Whenever the head of any such department, agency, or instrumentality submits a report pursuant to section 552a(o) of title 5, United States Code, a copy of such report shall be transmitted to the Commission.

(B) In carrying out its functions and exercising its powers under this section, the Commission may accept from any such department, agency, independent instrumentality, or other person any individually identifiable data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such informa-

tion, it shall assure that the information is used only for the purpose for which it is provided, and upon completion of that purpose such information shall be destroyed or returned to such department, agency, independent instrumentality, or person from which it is obtained, as appropriate.

(3) The Commission shall have the power to—

(A) appoint and fix the compensation of an executive director, and such additional staff personnel as may be necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of such title; and

(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code.

The Commission may delegate any of its functions to such personnel of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(4) The Commission is authorized—

(A) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(B) to enter into contracts or other arrangements or modifications thereof, with any government, any department, agency, or independent instrumentality of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(C) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529); and

(D) to take such other action as may be necessary to carry out its functions under this section.

(f)(1) Each member of the Commission who is an officer or employee of the United States shall serve without additional compensation, but shall continue to receive the salary of his regular position when engaged in the performance of the duties vested in the Commission.

(2) A member of the Commission other than one to whom paragraph (1) applies shall receive per diem at the maximum daily rate for GS–18 of the General Schedule

when engaged in the actual performance of the duties vested in the Commission.

(3) All members of the Commission shall be reimbursed for travel, subsistence, and other necessary expenses incurred by them in the performance of the duties vested in the Commission.

(g) The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this section. The Commission shall make a final report to the President and to the Congress on its findings pursuant to the study required to be made under subsection (b)(1) of this section not later than two years from the date on which all of the members of the Commission are appointed. The Commission shall cease to exist thirty days after the date on which its final report is submitted to the President and the Congress.

(h)(1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Com-

mission under false pretenses shall be fined not more than $5,000.

SEC. 6. The Office of Management and Budget shall—

(1) develop guidelines and regulations for the use of agencies in implementing the provisions of section 552a of title 5, United States Code, as added by section 3 of this Act; and

(2) provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies.

SEC. 7. (a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) The provisions of paragraph (1) of this subsection shall not apply with respect to—

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

SEC. 8. The provisions of this Act shall be effective on and after the date of enactment, except that the amendments made by sections 3 and 4 shall become effective 270 days following the day on which this Act is enacted.

SEC. 9. There is authorized to be appropriated to carry out the provisions of section 5 of this Act for fiscal years 1975, 1976, and 1977 the sum of $1,500,000, except that not more than $750,000 may be expended during any such fiscal year.

Amend the amendment of the House to the title so as to read: "An Act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes."

Attest:

Secretary.

In the House of Representatives, U. S.,

December 18, 1974.

Resolved, That the House agree to the amendments of the Senate to the amendments of the House to bill (S. 3418) entitled "An Act to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes", with the following

AMENDMENTS:

(1) Page 16, strike out lines 1 through 10, inclusive, and insert:

"(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

"(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(2) Page 24, strike out all after line 10 over to and including line 24 on page 25, and insert:

"*(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b) (1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c) (1) and (2), (e)(4) (A) through (F), (e) (6), (7), (9), (10), and (11), and (i) if the system of records is—*

"*(1) maintained by the Central Intelligence Agency; or*

"*(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition*

of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(3) Page 42, strike out lines 11 through 21, and insert:

(h)(1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Commission under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

Attest:

Public Law 93-579
93rd Congress, S. 3418
December 31, 1974

An Act

To amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Privacy Act of 1974". Privacy Act of 1974. 5 USC 552a note.

SEC. 2. (a) The Congress finds that— Congressional findings. 5 USC 552a note.

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to— Statement of purpose.

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

88 STAT. 1896

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section: 88 STAT. 1897

5 USC 552a. **"§ 552a. Records maintained on individuals**

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

5 USC 552.

"(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

"(6) the term 'statistical record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13; and

13 USC 8.

"(7) the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) required under section 552 of this title;

"(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which

maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

"(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

"(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

"(11) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; Personal review.

"(2) permit the individual to request amendment of a record pertaining to him and— Amendment request.

"(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

"(B) promptly, either—

"(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason

for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

Review.

"(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

Notation of dispute.

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

"(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

"(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

Publication in Federal Register.

"(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

"(I) the categories of sources of records in the system;

"(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

"(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

"(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

"(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance; Rules of conduct.

"(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; and Confidentiality of records.

"(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency. Publication in Federal Register.

"(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall— 5 USC 553.

"(1) establish procedures whereby an individual can be notified

in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

Fees.

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

Publication in Federal Register.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency

"(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

"(B) refuses to comply with an individual request under subsection (d)(1) of this section;

"(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

"(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

Jurisdiction.

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

Amendment of record.

"(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

Injunction.

"(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of

any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of— Damages.

"(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

"(h) Rights of Legal Guardians.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) Criminal Penalties.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

"(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

"(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

"(j) General Exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through 5 USC 553.

(F), (e)(5), (7), (9), (10), and (11), and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

5 USC 553.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I) and (f) of this section if the system of records is—

5 USC 552.

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

18 USC 3056.

"(4) required by statute to be maintained and used solely as statistical records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the

Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553 (c) of this title, the reasons why the system of records is to be exempted from a provision of this section. 5 USC 553.

"(l)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section. 44 USC 3103.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register. Publication in Federal Register.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

"(m) GOVERNMENT CONTRACTORS.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

"(n) MAILING LISTS.—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

"(o) REPORT ON NEW SYSTEMS.—Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such Notice to Congress and OMB.

proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

Report to Speaker of the House and President of the Senate.

"(p) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

5 USC 552.

(q) EFFECT OF OTHER LAWS.—No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.".

5 USC prec. 500.

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Records about individuals."

immediately below:

"552. Public information; agency rules, opinions, orders, and proceedings.".

Privacy Protection Study Commission. Establishment. 5 USC 552a note. Membership.

SEC. 5. (a)(1) There is established a Privacy Protection Study Commission (hereinafter referred to as the "Commission") which shall be composed of seven members as follows:

(A) three appointed by the President of the United States,

(B) two appointed by the President of the Senate, and

(C) two appointed by the Speaker of the House of Representatives.

Members of the Commission shall be chosen from among persons who, by reason of their knowledge and expertise in any of the following areas—civil rights and liberties, law, social sciences, computer technology, business, records management, and State and local government—are well qualified for service on the Commission.

(2) The members of the Commission shall elect a Chairman from among themselves.

Vacancies.

(3) Any vacancy in the membership of the Commission, as long as there are four members in office, shall not impair the power of the Commission but shall be filled in the same manner in which the original appointment was made.

(4) A quorum of the Commission shall consist of a majority of the members, except that the Commission may establish a lower number as a quorum for the purpose of taking testimony. The Commission is authorized to establish such committees and delegate such authority to them as may be necessary to carry out its functions. Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information necessary to the performance of their functions, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or a member designated by the Chairman to be acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, other persons, and the public, and, on behalf of the Commission, shall see to the faithful execution of the administrative policies and decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

(5) (A) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress. Budget requests.

(B) Whenever the Commission submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress. Legislative recommendations.

(b) The Commission shall—

(1) make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information; and Study.

(2) recommend to the President and the Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information. Ante, p. 1897.

(c) (1) In the course of conducting the study required under subsection (b) (1) of this section, and in its reports thereon, the Commission may research, examine, and analyze—

(A) interstate transfer of information about individuals that is undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results in a violation of the implied or explicitly recognized confidentiality of such information.

(2) (A) The Commission may include in its examination personal information activities in the following areas: medical; insurance; education; employment and personnel; credit, banking and financial institutions; credit bureaus; the commercial reporting industry; cable television and other telecommunications media; travel, hotel and entertainment reservations; and electronic check processing.

(B) The Commission shall include in its examination a study of—

(i) whether a person engaged in interstate commerce who maintains a mailing list should be required to remove an individual's name and address from such list upon request of that individual;

(ii) whether the Internal Revenue Service should be prohibited from transfering individually indentifiable data to other agencies and to agencies of State governments;

(iii) whether the Federal Government should be liable for general damages incurred by an individual as the result of a willful or intentional violation of the provisions of sections 552a (g) (1) (C) or (D) of title 5, United States Code; and

Ante, p. 1897.

(iv) whether and how the standards for security and confidentiality of records required under section 552a (e) (10) of such title should be applied when a record is disclosed to a person other than an agency.

Religious organizations, exception.

(C) The Commission may study such other personal information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

Guidelines for study.

(3) In conducting such study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) examine the standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information; and

(D) to the maximum extent practicable, collect and utilize findings, reports, studies, hearing transcripts, and recommendations of governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission.

(d) In addition to its other functions the Commission may—

(1) request assistance of the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out its functions under this Act;

(2) upon request, assist Federal agencies in complying with the requirements of section 552a of title 5, United States Code;

(3) determine what specific categories of information, the collection of which would violate an individual's right of privacy, should be prohibited by statute from collection by Federal agencies; and

(4) upon request, prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation.

(e) (1) The Commission may, in carrying out its functions under this section, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Com-

mission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2)(A) Each department, agency, and instrumentality of the executive branch of the Government is authorized to furnish to the Commission, upon request made by the Chairman, such information, data, reports and such other assistance as the Commission deems necessary to carry out its functions under this section. Whenever the head of any such department, agency, or instrumentality submits a report pursuant to section 552a (o) of title 5, United States Code, a copy of such report shall be transmitted to the Commission.

Reports, transmittal to Commission. Ante, p. 1897.

(B) In carrying out its functions and exercising its powers under this section, the Commission may accept from any such department, agency, independent instrumentality, or other person any individually indentifiable data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall assure that the information is used only for the purpose for which it is provided, and upon completion of that purpose such information shall be destroyed or returned to such department, agency, independent instrumentality, or person from which it is obtained, as appropriate.

(3) The Commission shall have the power to——

(A) appoint and fix the compensation of an executive director, and such additional staff personnel as may be necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of such title; and

5 USC 5101, 5331.

5 USC 5332 note.

(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code.

The Commission may delegate any of its functions to such personnel of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(4) The Commission is authorized—

(A) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

Rules and regulations.

(B) to enter into contracts or other arrangements or modifications thereof, with any government, any department, agency, or independent instrumentality of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(C) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529); and

(D) to take such other action as may be necessary to carry out its functions under this section.

Compensation.

(f)(1) Each [the] member of the Commission who is an officer or employee of the United States shall serve without additional compensation, but shall continue to receive the salary of his regular position when engaged in the performance of the duties vested in the Commission.

Per diem.

(2) A member of the Commission other than one to whom paragraph (1) applies shall receive per diem at the maximum daily rate for GS-18 of the General Schedule when engaged in the actual performance of the duties vested in the Commission.

5 USC 5332 note.

Travel expenses.

(3) All members of the Commission shall be reimbursed for travel, subsistence, and other necessary expenses incurred by them in the performance of the duties vested in the Commission.

Report to President and Congress.

(g) The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this section. The Commission shall make a final report to the President and to the Congress on its findings pursuant to the study required to be made under subsection (b)(1) of this section not later than two years from the date on which all of the members of the Commission are appointed. The Commission shall cease to exist thirty days after the date on which its final report is submitted to the President and the Congress.

Penalties.

(h)(1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Commission under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

5 USC 552a note.

SEC. 6. The Office of Management and Budget shall—

(1) develop guidelines and regulations for the use of agencies in implementing the provisions of section 552a of title 5, United States Code, as added by section 3 of this Act; and

Ante, p. 1897.

(2) provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies.

5 USC 552a note.

SEC. 7. (a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to—

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Effective date.
5 USC 552a note.

SEC. 8. The provisions of this Act shall be effective on and after the date of enactment, except that the amendments made by sections 3 and 4 shall become effective 270 days following the day on which this Act is enacted.

Appropriation.
5 USC 552a note.

SEC. 9. There is authorized to be appropriated to carry out the provisions of section 5 of this Act for fiscal years 1975, 1976, and 1977 the sum of $1,500,000, except that not more than $750,000 may be expended during any such fiscal year.

Approved December 31, 1974.

LEGISLATIVE HISTORY:

HOUSE REPORT No. 93-1416 accompanying H.R. 16373 (Comm. on Government Operations).
SENATE REPORT No. 93-1183 (Comm. on Government Operations).
CONGRESSIONAL RECORD, Vol. 120 (1974):
Nov. 21, considered and passed Senate.
Dec. 11, considered and passed House, amended, in lieu of H.R. 16373.
Dec. 17, Senate concurred in House amendment with amendments.
Dec. 18, House concurred in Senate amendments.
WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 11, No. 1:
Jan. 1, Presidential statement.

PART 2—ADDITIONAL PRIVACY LEGISLATION

Calendar No. 701

93D CONGRESS
2D SESSION

S. 1688

[Report No. 93–724]

IN THE SENATE OF THE UNITED STATES

MAY 2, 1973

Mr. ERVIN (for himself, Mr. ABOUREZK, Mr. BAKER, Mr. BAYH, Mr. BEALL, Mr. BENNETT, Mr. BIBLE, Mr. BROOKE, Mr. BURDICK, Mr. HARRY F. BYRD, JR., Mr. CHURCH, Mr. FANNIN, Mr. FONG, Mr. GOLDWATER, Mr. GRAVEL, Mr. GURNEY, Mr. HANSEN, Mr. HASKELL, Mr. HATFIELD, Mr. HATHAWAY, Mr. HRUSKA, Mr. HUMPHREY, Mr. INOUYE, Mr. MANSFIELD, Mr. MCGEE, Mr. MCGOVERN, Mr. METCALF, Mr. MONDALE, Mr. MOSS, Mr. MUSKIE, Mr. NELSON, Mr. PACKWOOD, Mr. PELL, Mr. PERCY, Mr. RANDOLPH, Mr. SCOTT of Pennsylvania, Mr. STAFFORD, Mr. TAFT, Mr. THURMOND, Mr. TUNNEY, and Mr. WILLIAMS) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

MARCH 4, 1974

Reported by Mr. ERVIN, without amendment

A BILL

To protect the civilian employees of the executive branch of the United States Government in the enjoyment of their constitutional rights and to prevent unwarranted governmental invasions of their privacy.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. It shall be unlawful for any officer of any executive department or any executive agency of the United States Government, or for any person acting or purporting to act under his authority, to do any of the following things:

(a) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency, or any person seeking employment in the executive branch of the United States Government, to disclose his race, religion, or national origin, or the race, religion, or national origin of any of his forebears: *Provided, however,* That nothing contained in this subsection shall be construed to prohibit inquiry concerning the citizenship of any such employee or person if his citizenship is a statutory condition of his obtaining or retaining his employment: *Provided further,* That nothing contained in this subsection shall be construed to prohibit inquiry concerning the national origin or citizenship of any such employee or person or of his forebears, when such inquiry is deemed necessary or advisable to determine suitability for assignment to activities or undertakings related to the national security within the United States or to activities or undertakings of any nature outside the United States.

(b) To state or intimate, or to attempt to state or intimate, to any civilian employee of the United States serving in the department or agency that any notice will be taken of his attendance or lack of attendance at any assemblage, discussion, or lecture held or called by any officer of the executive branch of the United States Government, or by any person acting or purporting to act under his authority, or by any

63-619 O - 76 - 34

outside parties or organizations to advise, instruct, or indoctrinate any civilian employee of the United States serving in the department or agency in respect to any matter or subject other than the performance of official duties to which he is or may be assigned in the department or agency, or the development of skills, knowledge, or abilities which qualify him for the performance of such duties: *Provided, however*, That nothing contained in this subsection shall be construed to prohibit taking notice of the participation of a civilian employee in the activities of any professional group or association.

(c) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to participate in any way in any activities or undertakings unless such activities or undertakings are related to the performance of official duties to which he is or may be assigned in the department or agency, or to the development of skills, knowledge, or abilities which qualify him for the performance of such duties.

(d) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to make any report concerning any of his activities or undertakings unless such activities or undertakings are related to the performance of official duties to which he is or may be assigned in the

department or agency, or to the development of skills, knowledge, or abilities which qualify him for the performance of such duties, or unless there is reason to believe that the civilian employee is engaged in outside activities or employment in conflict with his official duties.

(e) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency, or any person applying for employment as a civilian employee in the executive branch of the United States Government, to submit to any interrogation or examination or to take any psychological test which is designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters: *Provided, however,* That nothing contained in this subsection shall be construed to prevent a physician from eliciting such information or authorizing such tests in the diagnosis or treatment of any civilian employee or applicant where such physician deems such information necessary to enable him to determine whether or not such individual is suffering from mental illness: *Provided further, however,* That this determination shall be made in individual cases and not pursuant to general practice or regulation governing the examination of employees or

applicants according to grade, agency, or duties: *Provided further, however,* That nothing contained in this subsection shall be construed to prohibit an officer of the department or agency from advising any civilian employee or applicant of a specific charge of sexual misconduct made against that person, and affording him an opportunity to refute the charge.

(f) To require or request, or attempt to require or request, any civilian employee of the United States serving in the department or agency, or any person applying for employment as a civilian employee in the executive branch of the United States Government, to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

(g) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to support by personal endeavor or contribution of money or any other thing of value the nomination or the election of any person or group of persons to public office in the Government of the United States or of any State, district, Commonwealth, territory, or possession of the United States, or to attend any meeting held to promote or support the activities or undertakings of any political

party of the United States or of any State, district, Commonwealth, territory, or possession of the United States.

(h) To coerce or attempt to coerce any civilian employee of the United States serving in the department or agency to invest his earnings in bonds or other obligations or securities issued by the United States or any of its departments or agencies, or to make donations to any institution or cause of any kind: *Provided, however,* That nothing contained in this subsection shall be construed to prohibit any officer of any executive department or any executive agency of the United States Government, or any person acting or purporting to act under his authority, from calling meetings and taking any action appropriate to afford any civilian employee of the United States the opportunity voluntarily to invest his earnings in bonds or other obligations or securities issued by the United States or any of its departments or agencies, or voluntarily to make donations to any institution or cause.

(i) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to disclose any items of his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family or household: *Provided, however,* That this subsection shall not apply to any civilian

employee who has authority to make any final determination with respect to the tax or other liability of any person, corporation, or other legal entity to the United States, or claims which require expenditure of moneys of the United States: *Provided further, however*, That nothing contained in this subsection shall prohibit the Department of the Treasury or any other executive department or agency of the United States Government from requiring any civilian employee of the United States to make such reports as may be necessary or appropriate for the determination of his liability for taxes, tariffs, custom duties, or other obligations imposed by law.

(j) To require or request, or to attempt to require or request, any civilian employee of the United States embraced within the terms of the proviso in subsection (i) to disclose any items of his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family or household other than specific items tending to indicate a conflict of interest in respect to the performance of any of the official duties to which he is or may be assigned.

(k) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency, who is under investigation for

misconduct, to submit to interrogation which could lead to disciplinary action without the presence of counsel or other person of his choice, if he so requests: *Provided, however,* That a civilian employee of the United States serving in the Central Intelligence Agency or the National Security Agency may be accompanied only by a person of his choice who serves in the agency in which the employee serves, or by counsel who has been approved by the agency for access to the information involved.

(l) To discharge, discipline, demote, deny promotion to, relocate, reassign, or otherwise discriminate in regard to any term or condition of employment of, any civilian employee of the United States serving in the department or agency, or to threaten to commit any of such acts, by reason of the refusal or failure of such employee to submit to or comply with any requirement, request, or action made unlawful by this Act, or by reason of the exercise by such civilian employee of any right granted or secured by this Act.

SEC. 2. It shall be unlawful for any officer of the United States Civil Service Commission, or for any person acting or purporting to act under his authority, to do any of the following things:

(a) To require or request, or to attempt to require or request, any executive department or any executive agency

of the United States Government, or any officer or employee serving in such department or agency, to violate any of the provisions of section 1 of this Act.

(b) To require or request, or to attempt to require or request, any person seeking to establish civil service status or eligibility for employment in the executive branch of the United States Government, or any person applying for employment in the executive branch of the United States Government, or any civilian employee of the United States serving in any department or agency of the United States Government, to submit to any interrogation or examination or to take any psychological test which is desgined to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters: *Provided, however,* That nothing contained in this subsection shall be construed to prevent a physician from eliciting such information or authorizing such tests in the diagnosis or treatment of any civilian employee or applicant where such physician deems such information necessary to enable him to determine whether or not such individual is suffering from mental illness: *Provided further, however,* That this determination shall be made in individual cases and not pursuant to general practice or regulation governing the exami-

nation of employees or applicants according to grade, agency, or duties: *Provided, further, however,* That nothing contained in this subsection shall be construed to prohibit an officer of the Civil Service Commission from advising any civilian employee or applicant on a specific charge of sexual misconduct made against that person, and affording him an opportunity to refute the charge.

(c) To require or request, or to attempt to require or request, any person seeking to establish civil service status or eligibility for employment in the executive branch of the United States Government, or any person applying for employment in the executive branch of the United States Government, or any civilian employee of the United States serving in any department or agency of the United States Goverment, to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

SEC. 3. It shall be unlawful for any commissioned officer, as defined in section 101 of title 10, United States Code, or any member of the Armed Forces acting or purporting to act under his authority, to require or request, or to attempt to require or request, any civilian employee of the executive branch of the United States Government under his authority

or subject to his supervision to perform any of the acts or submit to any of the requirements made unlawful by section 1 of this Act.

SEC. 4. Whenever any officer of any executive department or any executive agency of the United States Government, or any person acting or purporting to act under his authority, or any commissioned officer as defined in section 101 of title 10, United States Code, or any member of the Armed Forces acting or purporting to act under his authority, violates or threatens to violate any of the provisions of section 1, 2, or 3 of this Act, any civilian employee of the United States serving in any department or agency of the United States Government, or any person applying for employment in the executive branch of the United States Government, or any person seeking to establish civil service status or eligibility for employment in the executive branch of the United States Government, affected or aggrieved by the violation or threatened violation, may bring a civil action in his own behalf or in behalf of himself and others similarly situated, against the offending officer or person in the United States district court for the district in which the violation occurs or is threatened, or the district in which the offending officer or person is found, or in the United States District Court for the District of Columbia, to prevent the threatened violation or to obtain redress against the

consequences of the violation. The Attorney General shall defend all officers or persons sued under this section who acted pursuant to an order, regulation, or directive, or who, in his opinion, did not willfully violate the provisions of this Act. Such United States district court shall have jurisdiction to try and determine such civil action irrespective of the actuality or amount of pecuniary injury done or threatened, and without regard to whether the aggrieved party shall have exhausted any administrative remedies that may be provided by law, and to issue such restraining order, interlocutory injunction, permanent injunction, or mandatory injunction, or enter such other judgment or decree as may be necessary or appropriate to prevent the threatened violation, or to afford the plaintiff and others similarly situated complete relief against the consequences of the violation. With the written consent of any person affected or aggrieved by a violation or threatened violation of section 1, 2, or 3 of this Act, any employee organization may bring such action on behalf of such person, or may intervene in such action. For the purposes of this section, employee organizations shall be construed to include any brotherhood, council, federation, organization, union, or professional association made up in whole or in part of civilian employees of the United States and which has as one of its purposes dealing with departments, agencies, commissions,

and independent agencies of the United States concerning the condition and terms of employment of such employees.

SEC. 5. (a) There is hereby established a Board on Employees' Rights (hereinafter referred to as the "Board"). The Board shall be composed of three members, appointed by the President, by and with the advice and consent of the Senate. The President shall designate one member as chairman. No more than two members of the Board may be of the same political party. No member of the Board shall be an officer or employee of the United States Government.

(b) The term of office of each member of the Board shall be five years, except that (1) of those members first appointed, one shall serve for five years, one for three years, and one for one year, respectively, from the date of enactment of this Act, and (2) any member appointed to fill a vacancy occurring prior to the expiration of the term for which his predecessor was appointed shall be appointed for the remainder of such term.

(c) Members of the Board shall be compensated at the rate of $75 a day for each day spent in the work of the Board, and shall be paid actual travel expenses and per diem in lieu of subsistence expenses when away from their usual places of residence, as authorized by section 5703 of title 5, United States Code.

(d) Two members shall constitute a quorum for the transaction of business.

(e) The Board may appoint and fix the compensation of such officers, attorneys, and employees, and make such expenditures, as may be necessary to carry out its functions.

(f) The Board shall make such rules and regulations as shall be necessary and proper to carry out its functions.

(g) The Board shall have the authority and duty to receive and investigate written complaints from or on behalf of any person claiming to be affected or aggrieved by any violation or threatened violation of this Act and to conduct a hearing on each such complaint. Within ten days after the receipt of any such complaint, the Board shall furnish notice of the time, place, and nature of the hearing thereon to all interested parties. The Board shall render its final decision with respect to any complaint within thirty days after the conclusion of its hearing thereon.

(h) Officers or representatives of any Federal employee organization in any degree concerned with employment of the category in which any alleged violation of this Act occurred or is threatened shall be given an opportunity to participate in each hearing conducted under this section, through submission of written data, views, or arguments, and in the discretion of the Board, with opportunity for oral presentation. Government employees called upon by any

party or by any Federal employee organization to participate in any phase of any administrative or judicial proceeding under this section shall be free to do so without incurring travel cost or suffering loss in leave or pay; and all such employees shall be free from restraint, coercion, interference, intimidation, or reprisal in or because of their participation. Any periods of time spent by Government employees during such participation shall be held and considered to be Federal employment for all purposes.

(i) Insofar as consistent with the purposes of this section, the provisions of subchapter II of chapter 5 of title 5, United States Code, relating to the furnishing of notice and manner of conducting agency hearings, shall be applicable to hearings conducted by the Board under this section.

(j) If the Board shall determine after hearing that a violation of this Act has not occurred or is not threatened, the Board shall state its determination and notify all interested parties of such determination. Each such determination shall constitute a final decision of the Board for purposes of judicial review.

(k) If the Board shall determine that any violation of this Act has been committed or threatened by any civilian officer or employee of the United States, the Board shall immediately (1) issue and cause to be served on such officer or employee an order requiring such officer or employee

to cease and desist from the unlawful act or practice which constitutes a violation, (2) endeavor to eliminate any such unlawful act or practice by informal methods of conference, conciliation, and persuasion, and (3) may—

(A) (i) in the case of the first offense by any civilian officer or employee of the United States, other than any officer appointed by the President, by and with the advice and consent of the Senate, issue an official reprimand against such officer or employee or order the suspension without pay of such officer or employee from the position or office held by him for a period of not to exceed fifteen days, and (ii) in the case of a second or subsequent offense by any such officer or employee, order the suspension without pay of such officer or employee from the position or office held by him for a period of not to exceed thirty days or order the removal of such officer or employee from such position or office; and

(B) in the case of any offense by any officer appointed by the President, by and with the advice and consent of the Senate, transmit a report concerning such violation to the President and the Congress.

(l) If the Board shall determine that any violation of this Act has been committed or threatened by any officer of any of the Armed Forces of the United States, or any

person purporting to act under authority conferred by such officer, the Board shall (1) submit a report thereon to the President, the Congress, and the Secretary of the military department concerned, (2) endeavor to eliminate any unlawful act or practice which constitutes such a violation by informal methods of conference, conciliation, and persuasion, and (3) refer its determination and the record in the case to any person authorized to convene general courts-martial under section 822 (article 22) of title 10, United States Code. Thereupon such person shall take immediate steps to dispose of the matter under chapter 47 of title 10, United States Code (Uniform Code of Military Justice).

(m) Any party aggrieved by any final determination or order of the Board may institute, in the district court of the United States for the judicial district wherein the violation or threatened violation of this Act occurred, or in the United States District Court for the District of Columbia, a civil action for the review of such determination or order. In any such action, the court shall have jurisdiction to (1) affirm, modify, or set aside any determination or order made by the Board which is under review, or (2) require the Board to make any determination or order which it is authorized to make under subsection (k), but which it has refused to make. The reviewing court shall set aside any finding, conclusion, determination, or order of the Board as to which

complaint is made which is unsupported by substantial evidence on the record considered as a whole.

(n) The Board shall submit, not later than March 31 of each year, to the Senate and House of Representatives, respectively, a report on its activities under this section during the immediately preceding calendar year, including a statement concerning the nature of all complaints filed with it, its determinations and orders resulting from hearings thereon, and the names of all officers or employees of the United States with respect to whom any penalties have been imposed under this section.

(o) There are authorized to be appropriated sums necessary, not in excess of $100,000, to carry out the provisions of this section.

SEC. 6. Nothing contained in this Act shall be construed to prohibit an officer of the Central Intelligence Agency or of the National Security Agency from requesting any civilian employee or applicant to take a polygraph test, or to take a psychological test, designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters, or to provide a personal financial statement, if the Director of the Central Intelligence Agency or his designee or the Director of the National Security Agency or his designee makes a personal

63-619 O - 76 - 35

finding with regard to each individual to be so tested or examined that such test or information is required to protect the national security.

SEC. 7. No civilian employee of the United States serving in the Central Intelligence Agency or the National Security Agency, and no individual or organization acting in behalf of such employee, shall be permitted to invoke the provisions of sections 4 and 5 without first submitting a written complaint to the agency concerned about the threatened or actual violation of this Act and affording such agency one hundred and twenty days from the date of such complaint to prevent the threatened violation or to redress the actual violation: *Provided, however,* That nothing in this Act shall be construed to affect any existing authority of the Director of Central Intelligence under section 403(c), of title 50, United States Code, and any authorities available to the National Security Agency under section 833 of title 50, United States Code, to terminate the employment of any employee.

SEC. 8. Nothing in this Act shall be construed to affect in any way the authority of the Directors of the Central Intelligence Agency or the National Security Agency to protect or withhold information pursuant to statute or executive order. The personal certification by the Director of the agency that disclosure of any information is inconsistent with the provision of any statute or Executive order shall be conclusive and no such information shall be admissible in evi-

dence in any interrogation under section 1(k) or in any civil action under section 4 or in any proceeding or civil action under section 5.

SEC. 9. This Act shall not be applicable to the Federal Bureau of Investigation.

SEC. 10. Nothing contained in sections 4 and 5 shall be construed to prevent establishment of department and agency grievance procedures to enforce this Act, but the existence of such procedures shall not preclude any applicant or employee from pursuing the remedies established by this Act or any other remedies provided by law: *Provided, however,* That if under the procedures established, the employee or applicant has obtained complete protection against threatened violations or complete redress for violations, such action may be pleaded in bar in the United States district court or in proceedings before the Board on Employee Rights: *And provided further,* That if an employee elects to seek a remedy under either section 4 or section 5, he waives his right to proceed by an independent action under the remaining section.

SEC. 11. If any provision of this Act or the application of any provision to any person or circumstance shall be held invalid, the remainder of this Act or the application of such provision to persons or circumstances other than those as to which it is held invalid, shall not be affected.

Calendar No. 701

93D CONGRESS
1st Session

SENATE

REPORT
No. 93-724

PROTECTING PRIVACY AND THE RIGHTS OF FEDERAL EMPLOYEES

MARCH 4, 1974.—Ordered be to printed

Mr. ERVIN, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 1688]

The Subcommittee on Constitutional Rights to which was referred the bill S. 1688 to protect civilian employees of the executive branch of the U.S. Government in the enjoyment of their constitutional rights and to prevent unwarranted governmental invasions of their privacy, having considered the same, reports favorably thereon without amendments and recommends that the bill do pass.

S. 1688 is identical to S. 1438 as unanimously reported by the committee and unanimously approved by the Senate in the last Congress. The report on S. 1438 is therefore reprinted below as approved by the committee.

PURPOSE

The purpose of the bill is to prohibit indiscriminate executive branch requirements that employees and, in certain instances, applicants for Government employment disclose their race, religion, or national origin; attend Government-sponsored meetings and lectures or participate in outside activities unrelated to their employment; report on their outside activities or undertakings unrelated to their work; submit to questioning about their religion, personal relationships or sexual attitudes through interviews, psychological tests, or polygraphs; support political candidates or attend political meetings. The bill would make it illegal to coerce an employee to buy bonds or make charitable contributions. It prohibits officials from requiring him to disclose his own personal assets, liabilities, or expenditures, or those of any member of his family unless, in the case of certain specified employees, such items would tend to show a conflict of interest. It would provide a right to have a counsel or other person present, if the

employee wishes, at an interview which may lead to disciplinary proceedings. It would accord the right to a civil action in a Federal court for violation or threatened violation of the act, and it would establish a Board on Employees' Rights to receive and conduct hearings on complaints of violation of the act and to determine and administer remedies and penalties.

STATEMENT

The subcommittee has found a threefold need for this legislation. The first is the immediate need to establish a statutory basis for the preservation of certain rights and liberties of those who work for government now and those who will work for it in the future. The bill, therefore, not only remedies problems of today but looks to the future, in recognition of the almost certain enlargement of the scope of Federal activity and the continuing rise in the number of Americans employed by their Federal Government or serving it in some capacity.

Second, the bill meets the Federal Government's need to attract the best qualified employees and to retain them. As the former Chairman of the Civil Service Commission, Robert Ramspeck, testified:

> Today, the Federal Government affects the lives of every human being in the United States. Therefore, we need better people today, better qualified people, more dedicated people, in Federal service than we ever needed before. And we cannot get them if you are going to deal with them on the basis of suspicion, and delve into their private lives, because if there is anything the average American cherishes, it is his right of freedom of action, and his right to privacy. So I think this bill is hitting at an evil that has grown up, maybe not intended, but which is hurting the ability of the Federal Government to acquire the type of personnel that we must have in the career service.

Third is the growing need for the beneficial influence which such a statute would provide in view of the present impact of Federal policies, regulations and practices on those of State and local government and of private business and industry. An example of the interest demonstrated by governmental and private employers is the following comment by Allan J. Graham, secretary of the Civil Service Commission of the city of New York:

> It is my opinion, based on over 25 years of former Government service, including some years in a fairly high managerial capacity, that your bill, if enacted into law, will be a major step to stem the tide of "Big Brotherism," which constitutes a very real threat to our American way of life.
>
> In my present position as secretary of the Civil Service Commission of the city of New York, I have taken steps to propose the inclusion of several of the concepts of your bill into the rules and regulations of the city civil service commission.

Passage of the bill will signify congressional recognition of the threats to individual privacy posed by an advanced technology and by increasingly more complex organizations. Illustrating these trends is

the greatly expanded use of computers and governmental and private development of vast systems for the efficient gathering of information and for data storage and retrieval. While Government enjoys the benefit of these developments, there is at the same time an urgent need for defining the areas of individual liberty and privacy which should be exempt from the unwarranted intrustions facilitated by scientific techniques.

As Prof. Charles Reich of Yale Law School has stated, this bill "would be a significant step forward in defining the right of privacy today."

"One of the most important tasks which faces the Congress and State legislatures in the next decade is the protection of the citizen against invasion of privacy," states Prof. Stanley Anderson of the University of California, Santa Barbara. "No citizens," in his opinion, "are in more immediate danger of incursion into private affairs than Government employees. When enacted the bill will provide a bulwark of protection against such incursions."

The bill is based on several premises which the subcommittee investigation has proved valid for purposes of enacting this legislation. The first is that civil servants do not surrender the basic rights and liberties which are their due as citizens under the Constitution of the United States by their action in accepting Government employment. Chief among these constitutional protections is the first amendment, which protects the employee to privacy in his thoughts, beliefs and attitudes, to silence in his action and participation or his inaction and nonparticipation in community life and civic affairs. This principle is the essence of constitutional liberty in a free society.

The constitutional focus of the bill was emphasized by Senator Ervin in the following terms when he introduced S. 1035 on February 21, 1967:

> If this bill is to have any meaning for those it affects, or serve as a precedent for those who seek guidance in these matters, its purpose must be phrased in constitutional terms. Otherwise its goals will be lost.
>
> We must have as our point of reference the constitutional principles which guide every official act of our Federal Government. I believe that the Constitution, as it was drafted and as it has been implemented, embodies a view of the citizen as possessed of an inherent dignity and as enjoying certain basic liberties. Many current practices of Government affecting employees are unconstitutional; they violate not only the letter but the very spirit of the Constitution.
>
> I introduced this bill originally because I believe that, to the extent it has permitted or authorized unwarranted invasion of employee privacy and unreasonable restrictions on their liberty, the Federal Government has neglected its constitutional duty where its own employees are concerned, and it has failed in its role as the model employer for the Nation.
>
> Second, although it is a question of some dispute, I hold that Congress has a duty under the Constitution not only to consider the constitutionality of the laws it enacts, but to assure as far as possible that those in the executive branch

> responsible for administering the laws adhere to constitutional standards in their programs, policies, and administrative techniques.

The committee believes that it is time for Congress to forsake its reluctance to tell the executive branch how to treat its employees. When so many American citizens are subject to unfair treatment, to being unreasonably coerced or required without warrant to surrender their liberty, their privacy, or their freedom to act or not to act, to reveal or not to reveal information about themselves and their private thoughts and actions, then Congress has a duty to call a statutory halt to such practices. It has a duty to remind the executive branch that even though it might have to expend a little more time and effort to obtain some favored policy goal, the techniques and tools must be reasonable and fair.

Each section of the bill is based on evidence from many hundreds of cases and complaints showing that generally in the Federal service, as in any similar organizational situation, a request from a superior is equivalent to a command. This evidence refutes the argument that an employee's response to a superior's request for information or action is a voluntary response, and that an employee "consents" to an invasion of his privacy or the curtailment of his liberty. Where his employment opportunities are at stake, where there is present the economic coercion to submit to questionable practices which are contrary to our constitutional values, then the presence of consent or voluntarism may be open to serious doubt. For this reason the bill makes it illegal for officials to "request" as well as to "require" an employee to submit to certain inquiries or practices or to take certain actions.

Each section of the bill reflects a balancing of the interests involved: The interest of the Government in attracting the best qualified individuals to its service; and its interest in pursuing laudable goals such as protecting the national security, promoting equal employment opportunities, assuring mental health, or conducting successful bond-selling campaigns. There is, however, also the interest of the individual in protection of his rights and liberties as a private citizen. When he becomes an employee of his Government, he has a right to expect that the policies and practices applicable to him will reflect the best values of his society.

The balance of interests achieved assures him this right. While it places no absolute prohibition on Government inquiries, the bill does assure that restrictions on his rights and liberties as a Government employee are reasonable ones.

As Senator Bible stated:

> There is a line between what is Federal business and what is personal business, and Congress must draw that line. The right of privacy must be spelled out.

The weight of evidence, as Senator Fong has said: "points to the fact that the invasions of privacy under threats and coercion and economic intimidation are rampant in our Federal civil service system today. The degree of privacy in the lives of our civil servants is small enough as it is, and it is still shrinking with further advances in tech-

nical know-how. That these citizens are being forced by economic coercion to surrender this precious liberty in order to obtain and hold jobs is an invasion of privacy which should disturb every American. I, therefore, strongly believe that congressional action to protect our civil servants is long overdue."

The national president of the National Association of Internal Revenue Employees, Vincent Connery, told the Subcommittee of this proposal in the 89th Congress:

> Senate bill 3779 is soundly conceived and perfectly timed. It appears on the legislative scene during a season of public employee unrest, and a period of rapidly accelerating demand among Federal employees for truly first-class citizenship. For the first time within my memory, at least, a proposed bill holds out the serious hope of attaining such a citizenship. S. 3779, therefore, amply deserves the fullest support of all employee organizations, both public and private, federation affiliated, and independent alike.

Similar statements endorsing the broad purpose of the bill were made by many others, including the following witnesses:

John F. Griner, national president, American Federation of Government Employees.

E. C. Hallbeck, national president, United Federation of Postal Clerks.

Jerome Keating, president, National Association of Letter Carriers.

Kenneth T. Lyons, national president, National Association of Government Employees.

John A. McCart, operations director, Government Employees Council of AFL–CIO.

Hon. Robert Ramspeck, former Chairman, Civil Service Commission.

Vincent Jay, executive vice president, Federal Professional Association.

Francis J. Speh, president, 14th District Department, American Federation of Government Employees.

Lawrence Speiser, director, Washington office, American Civil Liberties Union.

Nathan Wolkomir, national president, National Federation of Federal Employees.

LEGISLATIVE HISTORY

Following is a chronological account of committee action on this legislation to date.

S. 1688 was preceded by S. 1438 of the 92d Congress, S. 782 of the 91st Congress, by S. 1035 of the 90th Congress, and by S. 3079 and S. 3703 of the 89th Congress.

Violations of rights covered by the bill as well as other areas of employee rights have been the subject of intensive hearings and investigation by the subcommittee for the last five Congresses.

In addition to investigation of individual cases, the Subcommittee on Constitutional Rights has conducted annual surveys of agency policies on numerous aspects of Government personnel practices. In

1965, pursuant to Senate Resolution 43, hearings were conducted on due process and improper use of information acquired through psychological testing, psychiatric examinations, and security and personnel interviews.

In a letter to the Chief Executive on August 3, 1966, the subcommittee chairman stated:

> For some time, the Constitutional Rights Subcommittee has received disturbing reports from responsible sources concerning violations of the rights of Federal employees. I have attempted to direct the attention of appropriate officials to these matters, and although replies have been uniformly courteous, the subcommittee has received no satisfaction whatsoever, or even any indication of awareness that any problem exists. The invasions of privacy have reached such alarming proportions and are assuming such varied forms that the matter demands your immediate and personal attention.
>
> The misuse of privacy-invading personality tests for personnel purposes has already been the subject of hearings by the subcommittee. Other matters, such as improper and insulting questioning during background investigations and due process guarantees in denial of security clearances have also been the subject of study. Other employee complaints, fast becoming too numerous to catalog, concern such diverse matters as psychiatric interviews; lie detectors; race questionnaires; restrictions on communicating with Congress; pressure to support political parties yet restrictions on political activities; coercion to buy savings bonds; extensive limitations on outside activities yet administrative influence to participate in agency-approved functions; rules for writing, speaking and even thinking; and requirements to disclose personal information concerning finances, property and creditors of employees and members of their families.

After describing in detail the operation of two current programs to illustrate the problems, Senator Ervin commented:

> Many of the practices now in extensive use have little or nothing to do with an individual's ability or his qualification to perform a job. The Civil Service Commission has established rules and examinations to determine the qualifications of applicants. Apparently, the Civil Service Commission and the agencies are failing in their assignment to operate a merit system for our Federal civil service.
>
> It would seem in the interest of the administration to make an immediate review of these practices and questionnaires to determine whether the scope of the programs is not exceeding your original intent and whether the violations of employee rights are not more harmful to your long-range goals than the personnel shortcuts involved.

* * * * * * *

Following this letter and others addressed to the Chairman of the Civil Service Commission and the Secretaries of other departments,

legislation to protect employee rights was introduced in the Senate. This proposal, S. 3703 was introduced by the chairman on August 9, 1966, and referred to the Judiciary Committee. On August 25, 1966, the chairman received unanimous consent to a request to add the names of 33 cosponsors to the bill. On August 26, 1966, he introduced a bill similar to S. 3703, containing an amendment reducing the criminal penalties provided in section 2. This bill, S. 3779, was also referred to the Judiciary Committee, and both S. 3703 and S. 3779 were then referred to the Subcommittee on Constitutional Rights.

Comments on the bill and on problems related to it were made by the chairman in the Senate on July 18, August 9, August 25, August 26, September 29, October 17 and 18, 1966, and on February 21, 1967.[1]

Hearings on S. 3779 were conducted before the subcommittee on September 23, 29, 30, and October 3, 4, and 5, 1966. Reporting to the Senate on these hearings, the subcommittee chairman made the following statement:

> The recent hearings on S. 3779 showed that every major employee organization and union, thousands of individual employees who have written Congress, law professors, the American Civil Liberties Union, and a number of bar associations agree on the need for statutory protections such as those in this measure.
>
> We often find that as the saying goes "things are never as bad as we think they are," but in this case, the hearings show that privacy invasions are worse than we thought they were. Case after case of intimidation, of threats of loss of job or security clearance were brought to our attention in connection with bond sales, and Government charity drives.
>
> Case after case was cited of privacy invasion and denial of due process in connection with the new financial disclosure requirements. A typical case is the attorney threatened with disciplinary action or loss of his job because he is both unable and unwilling to list all gifts, including Christmas presents from his family, which he had received in the past year. He felt this had nothing to do with his job. There was the supervisory engineer who was told by the personnel officer that he would have to take disciplinary action against the 25 professional employees in his division who resented being forced to disclose the creditors and financial interests of themselves and members of their families. Yet there are no procedures for appealing the decisions of supervisors and personnel officers who are acting under the Commission's directive. These are not isolated instances; rather, they represent a pattern of privacy invasion reported from almost every State.
>
> The subcommittee was told that supervisors are ordered to supply names of employees who attend PTA meetings and engage in Great Books discussions. Under one department's regulations, employees are requested to participate in specific community activities promoting local and Federal antipoverty, beautification, and equal employment programs; they are told to lobby in local city councils for fair housing

[1] See also, *Cong. Rec.* Comments.

ordinances, to go out and make speeches on any number of subjects, to supply flower and grass seed for beautification projects, and to paint other people's houses. When those regulations were brought to the subcommittee's attention several weeks ago, we were told that they were in draft form. Yet, we then discovered they had already been implemented and employees whose official duties had nothing to do with such programs were being informed that failure to participate would indicate an uncooperative attitude and would be reflected in their efficiency records.

The subcommittee hearings have produced ample evidence of the outright intimidation, arm twisting and more subtle forms of coercion which result when a superior is requested to obtain employee participation in a program. We have seen this in the operation of the bond sale campaign, the drives of charitable contributions, and the use of self-identification minority status questionnaires. We have seen it in the sanctioning of polygraphs, personality tests, and improper questioning of applicants for employment.

In view of some of the current practices reported by employee organizations and unions, it seems those who endorse these techniques for mind probing and thought control of employees have sworn hostility against the idea that every man has a right to be free of every form of tyranny over his mind; they forget that to be free a man must have the right to think foolish thoughts as well as wise ones. They forget that the first amendment implies the right to remain silent as well as the right to speak freely—the right to do nothing as well as the right to help implement lofty ideals.

It is not under this administration alone that there has been a failure to respect employee rights in a zeal to obtain certain goals. While some of the problems are new, others have been prevalent for many years with little or no administrative action taken to attempt to ameliorate them. Despite congressional concern, administrative officials have failed to discern patterns of practice in denial of rights. They seem to think that if they can belatedly remedy one case which is brought to the attention of the Congress, the public and the press, that this is enough—that the "heat" will subside. With glittering generalities, qualified until they mean nothing in substance, they have sought to throw Congress off the track in its pursuit of permanent corrective action. We have seen this in the case of personality testing, in the use of polygraphs, and all the practices which the bill would prohibit.

The Chairman of the Civil Service Commission informed the subcommittee that there is no need for a law to protect employee rights. He believes the answer is—

> to permit executive branch management and executive branch employees as individuals and through their unions, to work together to resolve these issues as part of their normal discourse.

It is quite clear from the fearful tenor of the letters and telephone calls received by the subcommittee and Members of Congress that there is no discourse and is not likely to be any discourse on these matters between the Commission and employees. Furthermore, there are many who do not even fall within the Commission's jurisdiction. For them, there is no appeal but to Congress.

As for the argument that the discourse between the unions and the Commission will remedy the wrongs, the testimony of the union representatives adequately demolishes that dream.

The typical attitude of those responsible for personnel management is reflected in Mr. Macy's answer that there may be instances where policy is not adhered to, but "There is always someone who doesn't get the word." Corrective administration action, he says, is fully adequate to protect employee rights.

Administrative action is not sufficient. Furthermore, in the majority of complaints, the wrong actually stems from the stated policy of the agency or the Commission. How can these people be expected to judge objectively the reasonableness and constitutionality of their own policies? This is the role of Congress, and in my opinion, Congress has waited too long as it is to provide the guidance that is desperately needed in these matters.

S. 1035, 90th Congress

On the basis of the subcommittee hearings, agency reports, and the suggestions of many experts, the bill was amended to meet legitimate objections to the scope and language raised by administrative witnesses and to clarify the intent of its cosponsors that it does not apply to the proper exercise of management authority and supervisory discretion, or to matters now governed by statute.

This amended version of S. 3779 was introduced in the Senate by the chairman on February 21, 1967, as S. 1035 with 54 cosponsors. It was considered by the Constitutional Rights Subcommittee and unanimously reported with amendments by the Judiciary Committee on August 21, 1967. [S. Rept. No. 534, 90th Cong. 1st Sess.] The proposal was considered by the Senate on September 13, 1967, and approved, with floor amendments, by a 79 to 4 vote. After absentee approvals were recorded, the record showed a total of 90 Members supported passage of the bill. The amendments adopted on the Senate floor deleted a complete exemption which the committee bill provided for the Federal Bureau of Investigation; instead, it was provided that the Federal Bureau of Investigation should be accorded the same limited exemptions provided for the Central Intelligence Agency and the National Security Agency. A provision was added to allow the three Directors to delegate the power to make certain personal findings required by section 6 of the bill.

Committee amendments to S. 1035, 90th Congress

1. Amendment to section 1(a) page 2, line 13:

> *Provided further*, That nothing contained in this subsection shall be construed to prohibit inquiry concerning the national origin of any such employee when such inquiry is deemed necessary or advisable to determine suitability for assignment to activities or undertakings related to the national

security within the United States or to activities or undertakings of any nature outside the United States.

2. Amendment to section 1(b), page 2, line 25 strike "to" (technical amendment.)

3. Delete section 1(e), page 4, lines 1–4 (prohibitions on patronizing business establishments) and renumber following sections as sections 1(e), (f), (g), (h), (i), (j), (k), and (l), respectively.

4. Delete section 4, page 10, lines 12–23 (criminal penalties), and renumber following sections as sections 4 and 5, respectively.

5. Amendment to section 1(f), page 4, line 25:

> *Provided further, however*, That nothing contained in this subsection shall be construed to prohibit an officer of the department or agency from advising any civilian employee or applicant of a specific charge of sexual misconduct made against that person, and affording him an opportunity to refute the charge.

6. Amendments to section 1(f), page 4, at lines 17 and 19, change "psychiatrist" to "physician".

7. Amendment to section 1(k), page 7, at line 10, change (j) to (i).

8. Amendment to section 2(b), page 9, at line 6 and line 9, change "psychiatrist" to "physician".

9. Amendment to section 2(b), page 9, at line 15:

> *Provided further, however*, That nothing contained in this subsection shall be construed to prohibit an officer of the Civil Service Commission from advising any civilian employee or applicant of a specific charge of sexual misconduct made against that person, and affording him an opportunity to refute the charge.

10. Amendment to section 5, page 11, line 21, insert after the word "violation." the following:

> The Attorney General shall defend all officers or persons sued under this section who acted pursuant to an order, regulation, or directive, or who, in his opinion, did not willfully violate the provisions of this Act.

11. Amendment to section 6(l), page 16, at line 24, strike "sign charges and specifications under section 830 (art. 30)" and insert in lieu thereof "convene general courts-martial under section 822 (art. 22)" (technical amendment).

12. Amendment to section 6(m), page 17, line 14, change subsection (j) to (k) (technical amendment).

13. Amendment, page 18, add new section 6:

> SEC. 6. Nothing contained in this Act shall be construed to prohibit an officer of the Central Intelligence Agency or of the National Security Agency from requesting any civilian employee or applicant to take a polygraph test, or to take a psychological test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or

conduct with respect to sexual matters, or to provide a personal financial statement, if the Director of the Central Intelligence Agency or the Director of the National Security Agency makes a personal finding with regard to each individual to be so tested or examined that such test or information is required to protect the national security.

14. Amendment, page 18, add new section 8, and renumber following section as section 9:

SEC. 8. Nothing contained in sections 4 and 5 shall be construed to prevent establishment of department and agency grievance procedures to enforce this Act, but the existence of such procedures shall not preclude any applicant or employee from pursuing the remedies established by this Act or any other remedies provided by law: *Provided, however*, That if under the procedures established, the employee or applicant has obtained complete protection against threatened violations or complete redress for violations, such action may be pleaded in bar in the United States District Court or in proceedings before the Board on Employees' Rights: *Provided further, however*, That if an employee elects to seek a remedy under either section 4 or section 5, he waives his right to proceed by an independent action under the remaining section.

Comparison of S. 1035, 90th Congress, as introduced, and S. 3779, 89th Congress

As introduced, the revised bill, S. 1035, differed from S. 3779 of the 89th Congress in the following respects:

1. The section banning requirements to disclose race, religion, or national origin was amended to permit inquiry on citizenship where it is a statutory condition of employment.

2. The provision against coercion of employees to buy bonds or make charitable donations was amended to make it clear that it does not prohibit calling meetings or taking any action appropriate to afford the employee the opportunity voluntarily to invest or donate.

3. A new section providing for administrative remedies and penalties establishes a Board on Employees' Rights to receive and conduct hearings on complaints of violation of the act, and to determine and administer remedies and penalties. There is judicial review of the decision under the Administrative Procedure Act.

4. A specific exemption for the Federal Bureau of Investigation is included.

5. Exceptions to the prohibitions on privacy-invading questions by examination, interrogations, and psychological tests are provided upon psychiatric determination that the information is necessary in the diagnosis and treatment of mental illness in individual cases, and provided that it is not elicited pursuant to general practice or regulation governing the examination of employees or applicants on the basis of grade, job, or agency.

6. The section prohibiting requirements to disclose personal financial information contains technical amendments to assure that only

persons with final authority in certain areas may be subject to disclosure requirements.

7. For those employees excluded from the ban on disclosure requirements, a new section (j), provides that they may only be required to disclose items tending to show a conflict of interest.

8. Military supervisors of civilian employees are included within the prohibitions of the bill, and violation of the act is made a punishable offense under the Uniform Code of Military Justice.

9. A new section 2 has been added to assure that the same prohibitions in section 1 on actions of department and agency officials with respect to employees in their departments and agencies apply alike to officers of the Civil Service Commission with respect to the employees and applicants with whom they deal.

10. Section (b) of S. 3779, relating to the calling or holding of meetings or lectures to indoctrinate employees, was deleted.

11. Sections (c), (d), and (e) of S. 3779—sections (b), (c), and (d) of S. 1035—containing prohibitions on requiring attendance at outside meetings, reports on personal activities and participation in outside activities, were amended to make it clear that they do not apply to the performance of official duties or to the development of skill, knowledge, and abilities which qualify the person for his duties or to participation in professional groups or associations.

12. The criminal penalties were reduced from a maximum of $500 and 6 months' imprisonment to $300 and 30 days.

13. Section (h) of S. 3779 prohibiting requirements to support candidates, programs, or policies of any political party was revised to prohibit requirements to support the nomination or election of persons or to attend meetings to promote or support activities or undertakings of any political party.

14. Other amendments of a technical nature.

S. 782, 91st Congress—Committee amendments

S. 782, as introduced by Senator Ervin with 54 cosponsors, was identical to S. 1035 of the 90th Congress as passed by the Senate. As amended in Committee, it was reported to the Senate on May 15, 1970, and passed by unanimous consent on May 19.

The Subcommittee met in executive session on July 22, 1969, to receive testimony from Richard Helms, Director of the Central Intelligence Agency and other agency representatives. On the basis of this testimony and after a number of meetings of subcommittee members with officials of the Central Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation, the language contained in the committee amendments was drafted and meets with the approval of the Directors of those agencies.

Amendments

1. Amendment to section 1(a), page 2, line 15 insert after the word "origin" the words "or citizenship" and after the word "employee", the words "or person, or his forebears".

2. Amendment to section 1(k), page 8, line 5 after the word "requests", strike the period and insert the following:

> : *Provided, however*, That a civilian employee of the United States serving in the Central Intelligence Agency, or the

National Security Agency may be accompanied only by a person of his choice who serves in the agency in which the employee serves or by counsel who has been approved by the agency for access to the information involved.

3. Amendment to section 6, page 18, lines 15 and 16 delete "or of the Federal Bureau of Investigation".

4. Amendment to section 6, page 18, line 25, and page 19, line 1 delete "or the Director of the Federal Bureau of Investigation or his designee".

5. On page 19, add a new section 7 as follows:

SEC. 7. No civilian employee of the United States serving in the Central Intelligence Agency or the National Security Agency, and no individual or organization acting in behalf of such employee, shall be permitted to invoke the provisions of sections 4 and 5 without first submitting a written complaint to the agency concerned about the threatened or actual violation of this Act and affording such agency 120 days from the date of such complaint to prevent the threatened violation or to redress the actual violation: *Provided, however,* That nothing in this Act shall be construed to affect any existing authority of the Director of Central Intelligence under 50 U.S.C. 403(c), and any authorities available to the National Security Agency under 50 U.S.C. 833 to terminate the employment of any employee.

6. On page 19, add a new section 8 as follows:

SEC. 8. Nothing in this act shall be construed to affect in any way the authority of the Directors of the Central Intelligence Agency or the National Security Agency to protect or withhold information pursuant to statute or executive order. The personal certification by the Director of the agency that disclosure of any information is inconsistent with the provision of any statute or executive order shall be conclusive and no such information shall be admissible in evidence in any interrogation under section 1(k) or in any civil action under section 4 or in any proceeding or civil action under section 5.

7. On page 19, add a new section 9 as follows:

SEC. 9. This act shall not be applicable to the Federal Bureau of Investigation.

8. On page 19, at line 5, renumber "SEC. 7" as "SEC. 10" and at line 20, renumber "SEC. 8" as "SEC. 11".

S. 1438, 92d Congress

As introduced by Senator Ervin with 53 cosponsors, S. 1438 was identical to S. 782 of the 91st Congress as unanimously reported by the Committee and unanimously approved by the Senate. S. 1438 was approved by the Committee without amendment on December 6, 1971, passed by the Senate by unanimous consent on December 8, 1971, and was referred to the House Post Office and Civil Service Committee. There a majority of the full committee voted to table the bill.

On August 1, 1972, upon a motion by Senator Ervin, the Committee added the text of S. 1438 as Title II of the House-passed bill H.R. 12652, extending the life of the Civil Rights Commission and expanding its jurisdiction to include a study of the rights of women. On August 4, 1972, the Senate unanimously passed H.R. 12652 as amended. This marked the fourth time in six years that the Senate had approved the provisions of the employee privacy bill.

The House rejected the Senate amendment and requested a conference. The Senate conferees stood by the Senate amendment until it became apparent that it might jeopardize passage of the entire legislation. When the Senate passed the Civil Rights Commission authorization, it accepted the conference committee's decision to delete Title II from the bill.

QUESTIONS ON RACE, RELIGION, AND NATIONAL ORIGIN

Many complaints received by the subcommittee concerned official requests or requirements that employees disclose their race, religion, or ethnic or national origin. This information has been obtained from employees through the systematic use of questionnaires or oral inquiries by supervisors.

Chief concern has focused on a policy inaugurated by the Civil Service Commission in 1966, under which present employees and future employees would be asked to indicate on a questionnaire whether they were "American Indian," "oriental," "Negro," "Spanish-American" or "none of these." Approximately 1.7 million employees were told to complete the forms, while some agencies including some in the Department of Defense continued their former practice of acquiring such information through the "head count" method. Although the Civil Service Commission directive stated that disclosure of such information was voluntary, complaints show that employees and supervisors generally felt it to be mandatory. Administrative efforts to obtain compliance included in some instances harassment, threats, and intimidation. Complaints in different agencies showed that employees who did not comply received airmail letters at their homes with new forms; or their names were placed on administrative lists for "follow-up" procedures, and supervisors were advised to obtain the information from delinquent employees by a certain date.

In the view of John McCart, representing the Government Employes' Council, AFL–CIO:

> When the Civil Service Commission and the regulations note that participation by the employee will be voluntary, this removes some of the onus of the encroachment on an individual's privacy. But in an organizational operation of the size and complexity of the Federal Government, it is just impossible to guarantee that each individual's right to privacy and confidentiality will be observed.
>
> In addition to that, there have been a large number of complaints from all kinds of Federal employees. In the interest of maintaining the rights of individual workers against the possibility of invading those rights, it would seem to us it would be better to abandon the present approach, because

63-619 O - 76 - 36

there are other alternatives available for determining whether that program is being carried out.

The hearing record contains numerous examples of disruption of employee-management relations, and of employee dissatisfaction with such official inquiries. Many told the subcommittee that they refused to complete the questionnaires because the matter was none of the Government's business; others, because of their mixed parentage, felt unable to state the information.

Since 1963, the policy of the American Civil Liberties Union on the method of collecting information about race has favored the head count wherever possible. Although the policy is presently under review, the subcommittee finds merit in the statement that:

> The collection and dissemination of information about race creates a conflict among several equally important civil liberties: the right of free speech and free inquiry, on the one hand, and the rights of privacy and of equality of treatment and of opportunity, on the other. The ACLU approves them all. But at this time in human history, when the principle of equality and nondiscrimination must be vigorously defended, it is necessary that the union oppose collection and dissemination of information regarding race, except only where rigorous justification is shown for such action. Where such collection and dissemination is shown to be justified, the gathering of information should be kept to the most limited form, wherever possible by use of the head count method, and the confidential nature of original records should be protected as far as possible.

Former Civil Service Commission Chairman Robert Ramspeck told the subcommittee:

> To consider race, color, religion, and national origin in making appointments, in promotions and retention of Federal employees is, in my opinion, contrary to the merit system. There should be no discrimination for or against minority persons in Federal Government employment.

As the hearings and complaints have demonstrated, the most telling argument against the use of such a questionnaire, other than the constitutional issue, is the fact that it does not work. This is shown by the admission by many employees that they either did not complete the forms or that they gave inaccurate data.

Mr. Macy informed the subcommittee:

> In the State of Hawaii the entire program was cut out because it had not been done there before, and it was inadvertently included in this one, and the feeling was that because of the racial composition there it would be exceedingly difficult to come up with any kind of identification along the lines of the card that we were distributing.

The Civil Service Commission on May 9 informed the subcommittee that it had "recently approved regulations which will end the use of voluntary self-identification of race as a means of obtaining minority

group statistics for the Federal work force." The Commission indicated its decision was based on the failure of the program to produce meaningful statistics. In its place the Commission will rely on supervisory reports based solely on observation, which would not be prohibited by the bill.

As Senator Fong stated:

> It should be noted that the bill would not bar head counts of employee racial extraction for statistical purposes by supervisors. However, the Congress has authorized the merit system for the Federal service and the race, national origin or religion of the individual or his forebears should have nothing to do with his ability or qualifications to do a job.

Section 1(a) of the bill was included to assure that employees will not again be subjected to such unwarranted invasion of ther privacy. It is designed to protect the merit system which Congress has authorized for the Federal service. Its passage will reaffirm the intent of Congress that a person's religion, race, and national or ethnic origin or that of his forebears have nothing to do with his ability or qualification to perform the requisite duties of a Federal position, or to qualify for a promotion.

By eliminating official authority to place the employee in a position in which he feels compelled to disclose this personal data, the bill will help to eliminate the basis for such complaints of invasion of privacy and discrimination as Congress has received for a number of years. It will protect Americans from the dilemma of the grandson of an American Indian who told the subcommittee that he had exercised his option and did not complete the minority status questionnaire. He did not know how to fill it out. Shortly thereafter he received a personal memorandum from his supervisor "requesting" him to complete a new questionnaire and "return it immediately." He wrote: "I personally feel that if I do not comply with this request (order), my job or any promotion which comes up could be in jeopardy."

The prohibitions in section 1(a) against official inquiries about religion, and in section 1(e) concerning religious beliefs and practices together constitute a bulwark to protect the individual's right to silence concerning his religious convictions and to refrain from an indication of his religious beliefs.

Referring to these two sections, Lawrence Speiser, director of the Washington office of the American Civil Liberties Union testified:

> These provisions would help, we hope, eliminate a constantly recurring problem involving those new Government employees who prefer to affirm their allegiance rather than swearing to it. All Government employees must sign an appointment affidavit and take an oath or affirmation of office.
>
> A problem arises not just when new employees enter Government employment but in all situations where the Government requires an oath, and there is an attempt made on the part of those who prefer to affirm. It is amazing the intransigence that arises on the part of clerks or those who require the filling out of these forms, or the giving of the statement in permitting individuals to affirm.

> The excuses that are made vary tremendously, either that the form can only be signed and they cannot accept a form in which "so help me God" is struck out, because that is an amendment, and they are bound by their instructions which do not permit any changes to be made on the forms at all.
>
> Also, in connection with the giving of oaths, I have had one case in which an investigator asked a young man this question: "For the purposes of administering the oath, do you believe in God?"
>
> It is to be hoped that the provisions of this bill would bar practices of that kind. The law should be clear at this time. Title I, United States Code, section 1 has a number of rules of construction, one of which says that wherever the word "oath" appears, that includes "affirmation," and wherever the word "swear" appears, that includes "affirm."
>
> This issue comes up sometimes when clerks will ask, "Why do you want to affirm? Do you belong to a religious group that requires an affirmation rather than taking an oath?" And unless the individual gives the right answer, the clerks won't let him affirm. It is clear under the *Torcaso* case that religious beliefs and lack of religious beliefs are equally entitled to the protection of the first amendment.

The objection has been raised that the prohibition against inquiries into race, religion, or national origin would hinder investigation of discrimination complaints. In effect, however, it is expected to aid rather than hinder in this area of the law, by decreasing the opportunities for discrimination initially. It does not hinder acquisition of the information elsewhere; nor does it prevent a person from volunteering the information if he wishes to supply it in filing a complaint or in the course of an investigation.

CONTROL OF EMPLOYEE OPINIONS, OUTSIDE ACTIVITIES

Reports have come to the subcommittee of infringements and threatened infringements on first amendment freedoms of employees: freedom to think for themselves free of Government indoctrination: freedom to choose their outside civic, social, and political activities as citizens free of official guidance; or even freedom to refuse to participate at all without reporting to supervisors.

Illustrative of the climate of surveillance the subcommittee has found was a 13-year-old Navy Department directive, reportedly similar to those in other agencies, warning employees to guard against "indirect remarks" and to seek "wise and mature" counsel within their agencies before joining civic or political associations.

In the view of the United Federation of Postal Clerks:

> Perhaps no other right is so essential to employee morale as the right to personal freedom and the absence of interference by the Government in the private lives and activities of its employees. Attempts to place prohibitions on the private associations of employees; mandatory reporting of social contacts with Members of Congress and the press; attempts to "orient" or "indoctrinate" Federal employees on

subjects outside their immediate areas of professional interest; attempts to "encourage" participation in outside activities or discourage patronage of selected business establishments and coercive campaigns for charitable donations are among the most noteworthy abuses of Federal employees' right to personal freedom.

An example of improper on-the-job indoctrination of employees about sociological and political matters was cited in his testimony by John Griner, president of the AFL–CIO affiliated American Federation of Government Employees:

> One instance of disregard of individual rights of employees as well as responsibility to the taxpayers, which has come to my attention, seems to illustrate the objectives of subsections (b), (c), and (d), of section 1 of the Ervin bill. It happened at a large field installation under the Department of Defense.
>
> The office chief called meetings of different groups of employees throughout the day * * *. A recording was played while employees listened about 30 minutes. It was supposedly a speech made at a university, which went deeply into the importance of integration of the races in this country. There was discussion of the United Nations—what a great thing it was—and how there never could be another world war. The person who reported this incident made this comment: "Think of the taxpayers' money used that day to hear that record." I think that speaks for itself.

Other witnesses were in agreement with Mr. Griner's view on the need for protecting employees now and in the future from any form of indoctrination on issues unrelated to their work. The issue was defined at hearings on S. 3779 in the following colloquy between the subcommittee chairman and Mr. Griner.

> If they are permitted to hold sessions such as this on Government time and at Government expense, they might then also hold sessions as to whether or not we should be involved in the Vietnam war or whether we should not be, whether we should pull out or whether we should stay, and I think it could go to any extreme under those conditions.
>
> Of course, we are concerned with it, yes. But that is not a matter for the daily routine of work.
>
> Senator ERVIN. Can you think of anything which has more direful implications for a free America than a practice by which a government would attempt to indoctrinate any man with respect to a particular view on any subject other than the proper performance of his work?
>
> Mr. GRINER. I think if we attempted to do that we would be violating the individual's constitutional rights.
>
> Senator ERVIN. Is there any reason whatever why a Federal civil service employee should not have the same right to have his freedom of thought on all things under the sun outside of the restricted sphere of the proper performance of his work that any other American enjoys?
>
> Mr. GRINER. No, sir.

With one complaint of attempted indoctrination of employees at a Federal installation, a civil servant enclosed a memorandum taken from a bulletin board stating the time, place, and date of a lecture by a sociology professor on the subject of the importance of racial integration. Attendance was to be voluntary but the notice stated that a record would be made of those attending or not attending.

Concerning such a practice, one witness commented: "If I had been a Federal employee and I cared anything about my job, I would have been at that lecture."

Employees of an installation in Pennsylvania complained of requirements to attend film lectures on issues of the cold war.

Witnesses agreed that taking notice of attendance at such meetings constituted a form of coercion to attend. Section 1(b) will eliminate such intimidation. It leaves unaffected existing authority to use any appropriate means, including publicity, to provide employees information about meetings concerning matters such as charity drives and bond-selling campaigns.

Section (c) protests a basic constitutional right of the individual employee to be free of official pressure on him to engage in any civic or political activity or undertaking which might involve him as a private citizen, but which has no relation to his Federal employment. It preserves his freedom of thought and expression, including his right to keep silent, or to remain inactive.

This section will place a statutory bar against the recurrence of employee complaints such as the following received by a Member of the Senate:

> Dear Senator ———: On ———, 1966, a group of Treasury Department administrators were called to Miami for a conference led by ———, Treasury Personnel Officer, with regard to new revisions in chapter 713 of the Treasury Personnel Manual.
>
> Over the years the Treasury Department has placed special emphasis on the hiring of Negroes under the equal employment opportunity program, and considerable progress in that regard has been made. However, the emphasis of the present conference was that our efforts in the field of equal employment opportunity have not been sufficient. Under the leadership of President Johnson and based on his strong statement with regard to the need for direct action to cure the basic causes leading to discrimination, the Treasury Department has now issued specific instructions requiring all supervisors and line managers to become actively and aggressively involved in the total civil rights problem.
>
> The requirements laid down by chapter 713 and its appendix include participation in such groups as the Urban League, NAACP, et cetera (these are named specifically) and involvement in the total community action program, including open housing, integration of schools, et cetera.
>
> The policies laid down in this regulation, as verbally explained by the Treasury representatives at the conference, go far beyond any concept of employee personnel responsibility previously expressed. In essence, this regulation requires every Treasury manager or supervisor to become a

social worker, both during his official hours and on his own time. This was only tangentially referred to in the regulation and its appendages, but was brought out forcefully in verbal statements by Mr. ——— and ———. Frankly, this is tremendously disturbing to me and to many of the other persons with whom I have discussed the matter. We do not deny the need for strong action in the field of civil rights, but we do sincerely question the authority of our Government to lay out requirements to be met on our own time which are repugnant to our personal beliefs and desires.

The question was asked as to what disciplinary measures would be taken against individuals declining to participate in these community action programs. The reply was given by the equal employment officer, that such refusal would constitute an undesirable work attitude bordering on insubordination and should at the very least be reflected on the annual efficiency rating of the employee.

The principles expressed in these regulations and in this conference strike me as being of highly dangerous potential. If we, who have no connection with welfare or social programs, can be required to take time from our full-time responsibilities in our particular agencies and from the hours normally reserved for our own refreshment and recreation to work toward integration of white neighborhoods, integration of schools by artificial means, and to train Negroes who have not availed themselves of the public schooling available, then it would seem quite possible that under other leadership, we could be required to perform other actions which would actually be detrimental to the interests of our Nation.

* * * * *

Testifying on the issue of reporting outside activities, the American Civil Liberties Union representative commented:

To the extent that individuals are apprehensive they are going to have to, at some future time, tell the Government about what organizations they have belonged to or been associated with, that is going to inhibit them in their willingness to explore all kinds of ideas, their willingness to hear speakers, their willingness to do all kinds of things. That has almost as deadening an effect on free speech in a democracy as if the opportunities were actually cut off.

The feeling of inhibition which these kinds of questions cause is as dangerous, it seems to me, as if the Government were making actual edicts.

Witnesses gave other examples of invasion of employees' private lives which would be halted by passage of the bill.

In the southwest a division chief dispatched a buck slip to his group supervisors demanding: "the names * * * of employees * * * who are participating in any activities including such things as: PTA in integrated schools, sports activities which are inter-social, and such things as Great Books discussion groups which have integrated memberships."

* * * * * * *

In a Washington office of the Department of Defense, a branch chief by telephone asked supervisors to obtain from employees the names of any organizations they belonged to. The purpose apparently was to obtain invitations for Federal Government officials to speak before such organizations.

* * * * * * *

Reports have come to the subcommittee that the Federal Maritime Commission, pursuant to civil service regulations, requested employees to participate in community activities to improve the employability of minority groups, and to report to the chairman any outside activities.

* * * * * * *

In addition to such directives, many other instances involving this type of restriction have come to the attention of the subcommittee over a period of years. For example, some agencies have either prohibited flatly, or required employees to report, all contacts, social or otherwise, with Members of Congress or congressional staff members. In many cases reported to the subcommittee, officials have taken reprisals against employees who communicated with their Congressmen and have issued directives threatening such action.

* * * * * * *

The Civil Service Commission on its Form 85 for nonsensitive positions requires an individual to list: "Organizations with which affiliated (past and present) other than religious or political organizations or those with religious or political affiliations (if none, so state)."

* * * * * * *

PRIVACY INVASIONS IN INTERVIEWS, INTERROGATIONS, AND PERSONALITY TESTS

Although it does not outlaw all of the unwarranted personal prying to which employees and applicants are now subjected, section 1(e) of the reported bill will prohibit the more serious invasions of personal privacy reported. The subcommittee believes it will also result in limitations beyond its specific prohibitions by encouraging admistrative adherence to the principles it reflects.

It will halt mass programs in which, as a general rule, agency officials conduct interviews during which they require or request applicants or employees to reveal intimate details about their habits, thoughts, and attitudes on matters unrelated to their qualifications and ability to perform a job.

It will also halt individual interrogations such as that involving an 18-year-old college sophomore applying for a summer job as a secretary at a Federal department.

In the course of an interview with a department investigator, she was asked wide-ranging personal questions. For instance, regarding a boy whom she was dating, she was asked questions which denoted assumptions made by the investigator, such as:

> Did he abuse you?
> Did he do anything unnatural with you? You didn't get pregnant, did you?

There's kissing, petting, and intercourse, and after that, did he force you to do anything to him, or did he do anything to you?

The parent of this student wrote:

This interview greatly transcended the bounds of normal areas and many probing personal questions were propounded. Most questions were leading and either a negative or positive answer resulted in an appearance of self-incrimination. During this experience, my husband was on an unaccompanied tour of duty in Korea and I attempted alone, without success, to do battle with the Department.

I called and was denied any opportunity to review what had been recorded in my daughter's file. Likewise my daughter was denied any review of the file in order to verify or refute any of the record made by the State Department interviewer. This entire matter was handled as if applicants for State Department employment must subject themselves to the personal and intimate questions and abdicate all claims to personal rights and privileges.

As a result of this improper intrusion into my daughter's privacy which caused all great mental anguish, I had her application for employment withdrawn from the State Department. This loss of income made her college education that much more difficult.

Upon my husband's return, we discussed this entire situation and felt rather than subjecting her again to the sanctioned methods of Government investigation we would have her work for private industry. This she did in the summer of 1966, with great success and without embarrassing or humiliating Gestapo-type investigation.

Upon subcommittee investigation of this case, the Department indicated that this was not a unique case, because it used a "uniform policy in handling the applications of summer employees as followed with all other applicant categories." It stated that its procedure under Executive Order 10450 is a basic one "used by the Department and other executive agencies concerning the processing of any category of applicants who will be dealing with sensitive, classified material." Its only other comment on the case was to assure that "any information developed during the course of any of our investigations that is of a medical nature, is referred to our Medical Division for proper evaluation and judgment." In response to a request for copies of departmental guidelines governing such investigations and interviews, the subcommittee was told they were classified.

Section 1(e) would protect every employee and every civilian who offers his services to his Government from indiscriminate and unauthorized requests to submit to any test designed to elicit such information as the following:

My sex life is satisfactory,

I have never been in trouble because of my sex behavior.

Everything is turning out just like the prophets of the Bible said it would.

I loved my father.
I am very strongly attracted by members of my own sex.
I go to church almost every week.
I believe in the second coming of Christ.
I believe in a life hereafter.
I have never indulged in any unusual sex practices.
I am worried about sex matters.
I am very religious (more than most people).
I loved my mother.
I believe there is a Devil and a Hell in afterlife.
I believe there is a God.
Once in a while I feel hate toward members of my family whom I usually love.
I wish I were not bothered by thoughts about sex.

The subcommittee hearings in 1965 on "Psychological tests and constitutional rights" and its subsequent investigations support the need for such statutory prohibitions on the use of tests.

In another case, the subcommittee was told, a women was questioned for 6 hours "about every aspect of her sex life—real, imagined, and gossiped—with an intensity that could only have been the product of inordinately salacious minds."

The specific limitation on the three areas of questioning proscribed in S. 1035 in no way is intended as a grant of authority to continue or initiate the official eliciting of personal data from individuals on subjects not directly proscribed. It would prohibit investigators, or personnel, security and medical specialists from indiscriminately requiring or requesting the individual to supply, orally or through tests, data on religion, family, or sex. It does not prevent a physician from doing so if he has reason to believe the employee is "suffering from mental illness" and believes the information is necessary to make a diagnosis. Such a standard is stricter than the broad "fitness for duty" standard now generally applied by psychiatrists and physicians in the interviews and testing which an employee can be requested and required to undergo.

There is nothing in this section to prohibit an official from advising an individual of a specific charge of sexual misconduct and affording him an opportunity to refute the charge voluntarily.

POLYGRAPHS

Section 1(f) makes it unlawful for any officer of any executive department or agency or any person acting under his authority to require or request or attempt to require or request any civilian employee or any applicant for employment to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs, practices or concerning his attitude or conduct with respect to sexual matters. While this section does not eliminate the use of so-called lie detectors by Government, it assures that where such devices are used for these purposes it will be only in limited areas.

John McCart, representing the Government Employees Council of AFL–CIO, supported this section of the bill, citing a 1965 report by a special subcommittee of the AFL–CIO executive council that:

> The use of lie detectors violates basic considerations of human dignity in that they involve the invasion of privacy, self-incrimination, and the concept of guilt until proven innocent.

Congressional investigation[1] has shown that there is no scientific validation for the effectiveness or accuracy of lie detectors. Yet despite this and the invasion of privacy involved, lie detectors are being used or may be used in various agencies of the Federal Government for purposes of screening applicants or for pursuing investigations.

This section of the bill is based on complaints such as the following received by the subcommittee:

> When I graduated from college in 1965, I applied at NSA. I went to 2 days of testing, which apparently I passed because the interviewer seemed pleased and he told me that they could always find a place for someone with my type of degree.
>
> About 1 month later, I reported for a polygraph test at an office on Wisconsin Avenue in the District or just over the District line in Maryland. I talked with the polygraph operator, a young man around 25 years of age. He explained how the machine worked, etc. He ran through some of the questions before he attached the wires to me. Some of the questions I can remember are—
>
> "When was the first time you had sexual relations with a woman?
>
> "How many times have you had sexual intercourse?
>
> "Have you ever engaged in homosexual activities?
>
> "Have you ever engaged in sexual activities with an animal?
>
> "When was the first time you had intercourse with your wife?
>
> "Did you have intercourse with her before you were married? How many times?"
>
> He also asked questions about my parents, Communist activities, etc. I remember that I thought this thing was pretty outrageous, but the operator assured me that he asked everybody the same questions and he has heard all the answers before, it just didn't mean a thing to him. I wondered how he could ever get away with asking a girl those kinds of questions.
>
> When I was finished, I felt as though I had been in a 15 round championship boxing match. I felt exhausted. I made up my mind then and there that I wouldn't take the job even if they wanted me to take it. Also, I concluded that I would never again apply for a job with the Government, especially where they make you take one of these tests.

Commenting on this complaint, the subcommittee chairman observed:

---

[1] Hearings and reports on the use of polygraphs as "lie detectors," by the Federal Government before a Subcommittee of the House Committee on Government Operations, April 1964 through 1966.

Certainly such practices should not be tolerated even by agencies charged with security missions. Surely, the financial, scientific, and investigative resources of the Federal Government are sufficient to determine whether a person is a security risk, without strapping an applicant to a machine and subjecting him to salacious questioning. The Federal Bureau of Investigation does not use personality tests or polygraphs on applicants for employment. I fail to see why the National Security Agency finds them so fascinating.

COERCION TO BUY BONDS AND CONTRIBUTE TO CAUSES

The hearing record and subcommittee complaint files amply document the need for statutory protections against all forms of coercion of employees to buy bonds and contribute to causes. Involved here is the freedom of the individual to invest and donate his money as he sees fit, without official coercion. As the subcommittee chairman explained:

> It certainly seems to me that each Federal employee, like any other citizen in the United States, is the best judge of his capacity, in the light of his financial obligations, to participate or decide whether he will participate and the extent of his participation in a bond drive. That is a basic determination which he and he alone should make.
>
> I think there is an interference with fundamental rights when coercion of a psychological or economic nature is brought on a Federal employee, even to make him do right. I think a man has to have a choice of acting unwisely as well as wisely, if he is going to have any freedom at all.

The subcommittee has received from employees and their organizations numerous reports of intimidation, threats of loss of job, and security clearances and of denial of promotion for employees who do not participate to the extent supervisors wish. The hearing record contains examples of documented cases of reprisals, many of which have been investigated at the subcommittee's request and confirmed by the agency involved. It is apparent that policy statements and administrative rules are not sufficient to protect individuals from such coercion.

The president of the United Federation of Postal Clerks informed the subcommittee:

> Section 1, paragraph (i) of S. 3779 is particularly important to all Federal employees and certainly to our postal clerks. The extreme arm-twisting coercion, and pressure tactics exerted by some postmasters on our members earlier this year during the savings bond drive must not be permitted at any future time in the Government service.
>
> Our union received complaints from all over the country where low-paid postal clerks, most having the almost impossible problem of trying to support a family and exist on substandard wages, were practically being ordered to sign up for purchase of U.S. savings bonds, or else. The patriotism of our postal employees cannot be challenged. I recently was

advised that almost 75 percent of postal workers are veterans of the Armed Forces and have proven their loyalty and patriotism to this great country of ours on the battlefield in many wars. Yet, some postmasters questioned this patriotism and loyalty if any employee could not afford to purchase a savings bond during the drive.

The president of the National Association of Government Employees testified:

> We are aware of instances wherein employees were told that if they failed to participate in the bond program they would be frozen in their position without promotional opportunities.
>
> In another agency the names of individuals who did not participate were posted for all to see. We have been made aware of this situation for some years and we know that Congress has been advised of the many instances and injustices Federal employees faced concerning their refusal or inability to purchase bonds.
>
> Certainly, the Government, which has thousands of public relations men in its agencies and departments, should be capable of promoting a bond program that does not include the sledge-hammer approach.

Some concern has been expressed by officials of the United Community Funds and Councils of America, the American Heart Association, Inc., and other charitable organizations, that the bill would hamper their campaigns in Federal agencies.

For this reason, the bill contains a proviso to express the intent of the sponsors that officials may still schedule meetings and take any appropriate action to publicize campaigns and to afford employees the opportunity to invest or donate their money voluntarily. It is felt that this section leaves a wide scope for reasonable action in promoting bond selling and charity drives.

The bill will prohibit such practices as were reported to the subcommittee in the following complaints:

> We have not yet sold our former home and cannot afford to buy bonds while we have both mortgage payments and rental payments to meet. Yet I have been forced to buy bonds, as I was told the policy at this base is, "Buy bonds or by-by."
>
> In short, after moving 1,700 miles for the good of the Government, I was told I would be fired if I didn't invest my money as my employer directed. I cannot afford to buy bonds, but I can't afford to be fired even more.
>
> * * * * *
>
> Not only were we forced to buy bonds, but our superiors stood by the time clock with the blanks for the United Givers Fund, and refused to let us leave until we signed up. I am afraid to sign my name, but I am employed at * * *.
>
> * * * * *

A representative of the 14th District Department of the American Federation of Government Employees, Lodge 421, reported:

> The case of a GS–13 professional employee who has had the misfortune this past year of underwriting the expenses incurred by the last illness and death of both his mother and father just prior to this recent bond drive. This employee had been unofficially informed by his supervisor that he had been selected for a then existing GS–14 vacancy. When it became known that he was declining to increase his participation in the savings bond drive by increasing his payroll deduction for that purpose, he was informed that he might as well, in effect, kiss that grade 14 goodby.

DISCLOSURE OF ASSETS, DEBTS, AND PROPERTY

Sections (i) and (j) meet a need for imposing a reasonable statutory limitation on the extent to which an employee must reveal the details of his or his family's personal finances, debts, or ownership of property.

The subcommittee believes that the conflict-of-interest statutes, and the many other laws governing conduct of employees, together with appropriate implementing regulations, are sufficient to protect the Government from dishonest employees. More zealous informational activities on the part of management were recommended by witnesses in lieu of the many questionnaires now required.

The employee criticism of such inquiries was summarized as follows:

> There are ample laws on the statute books dealing with fraudulent employment, conflict of interest, etc. The invasion of privacy of the individual employee is serious enough, but the invasion of the privacy of family, relatives and children of the employee is an outrage against a free society.
>
> This forced financial disclosure has caused serious moral problems and feelings by employees that the agencies distrust their integrity. We do not doubt that if every employee was required to file an absolutely honest financial disclosure, that a few, though insignificant number of conflict-of-interest cases may result. However, the discovery of the few legal infractions could in no way justify the damaging effects of forced disclosures of a private nature. Further, it is our opinion that those who are intent on engaging in activities which result in a conflict of interest would hardly supply that information on a questionnaire or financial statement. Many employees have indicated that rather than subject their families to any such unwarranted invasion of their right to privacy, that they are seriously considering other employment outside of Government.

The bill will reduce to reasonable proportions such inquiries as the following questionnaire, which many thousands of employees have periodically been required to submit.

(Questionnaire follows:)

CONFIDENTIAL STATEMENT OF EMPLOYMENT AND FINANCIAL INTERESTS

(FOR USE BY REGULAR GOVERNMENT EMPLOYEES)

NAME (Last, First, Initial)	TITLE OF POSITION
DATE OF APPOINTMENT IN PRESENT POSITION	ORGANIZATION LOCATION (Operating agency), Bureau Division)

PART I. EMPLOYMENT AND FINANCIAL INTERESTS

List the names of all corporations, companies, firms, or other business enterprises, partnerships, nonprofit organizations, and educational, or other institutions: (a) with which you are connected as an employee, officer, owner, director, member, trustee, partner, adviser, or consultant, or (b) in which you have any continuing financial interests, through a pension or retirement plan, shared income, or other arrangement as a result of any current or prior employment or business or professional association; or (c) in which you have any financial interest through the ownership of stock, stock options, bonds, securities, or other arrangements including trusts. If none, write NONE.

NAME AND KIND OF ORGANIZATION (Use Part I designations where applicable)	ADDRESS	POSITION IN ORGANIZATION (Use Part I (a) designations, if applicable.	NATURE OF FINANCIAL INTEREST, e.g., STOCKS, PRIOR INCOME (Use Part I (b) & (c) designations if applicable)

PART II. CREDITORS

List the names of your creditors other than those to whom you may be indebted by reason of a mortgage on property which you occupy as a personal residence or to whom you may be indebted for current and ordinary household and living expenses such as household furnishings, automobile, education, vacation, and similar expenses. If none, write NONE.

NAME AND ADDRESS OF CREDITOR	CHARACTER OF INDEBTEDNESS, e.g., PERSONAL LOAN, NOTE, SECURITY

PART III. INTERESTS IN REAL PROPERTY

List your interest in real property or rights in lands, other than property which you occupy as a personal residence. If none, write NONE.

NATURE OF INTEREST, e.g., OWNERSHIP, MORTGAGE, LIEN, INVESTMENT TRUST	TYPE OF PROPERTY, e.g., RESIDENCE, HOTEL, APARTMENT, UNDEVELOPED LAND	ADDRESS (If rural, give RFD or county and State)

PART IV. INFORMATION REQUESTED OF OTHER PERSONS

If any information is to be supplied by other persons, e.g., trustee, attorney, accountant, relative, please indicate the name and address of such persons, the date upon which you requested that the information be supplied, and the nature of subject matter involved. If none, write NONE.

NAME AND ADDRESS	DATE OF REQUEST	NATURE OF SUBJECT MATTER

(THIS SPACE RESERVED FOR ADDITIONAL INSTRUCTIONS)

I certify that the statements I have made are true, complete, and correct to the best of my knowledge and belief.

MCM-478
63-48

(Date) (Signature)

The vagueness of the standards for requiring such a broad surrender of privacy is illustrated by the Civil Service Commission's regulation applying this to any employee whose duties have an "economic impact on a non-Federal enterprise."

Also eliminated will be questionnaires asking employees to list "all assets, or everything you and your immediate family own, including date acquired and cost or fair market value at acquisiton. (Cash in banks, cash anywhere else, due from others—loans, et cetera, automobiles, securities, real estate, cash surrender of life insurance; personal effects and household furnishings and other assets.)"

The view of the president of the United Federation of Postal Clerks reflected the testimony of many witnesses endorsing sections 1 (i) and (j) of the bill.

> If the conflict-of-interest questionnaire is of doubtful value in preventing conflict of interest, as we believe, we can only conclude that it does not meet the test of essentiality and that it should be proscribed as an unwarranted invasion of employee privacy. Such value as it may have in focusing employee attention upon the problem of conflict of interest and bringing to light honest oversights that may lead to conflict of interest could surely be achieved by drawing attention to the 26 or more laws pertaining to conflict of interest or by more zealous information activities on the part of management.

The complex problem of preserving the confidential nature of such reports was described by officials of the National Association of Internal Revenue Employees:

> The present abundance of financial questionnaires provides ample material for even more abusive personnel practices. It is almost inevitable that this confidential information cannot remain confidential. Typically, the financial questionnaire is filed with an employee's immediate supervisor. The net worth statements ultimately go into Inspection, but they pass through the hands of local personnel administrators. We have received a great number of disturbing reports—as have you—that this information about employees' private affairs is being used for improper purposes, such as enforced retirement and the like.

Inadequacies in agency procedures for obtaining such information from employees and for reviewing and storing it, are discussed in the Subcommittee report for the 89th Congress, 2d Session. Widely disparate attitudes and practices are also revealed in a Subcommittee study contained in the appendix of the printed hearings on S. 3779.

The bill will make such complaints as the following unnecessary in the future conduct of the Federal Government:

Dear Senator Ervin: I am writing to applaud the stand you have taken on the new requirement that Federal employees in certain grades and categories disclose their financial holdings to their immediate superior. Having been a civil service employee for 26 years, and advanced from GS–4 to GS–15, and been cleared for top secret during World War II, and because I currently hold a position that involves the dispositon of hundreds of thousands of the taxpayers' money, it is my conviction that my morality and trustworthiness are already a matter of record in the files of the Federal Government.

The requirement that my husband's financial assets be reported, as well as my own assets and those we hold jointly, was particularly offensive, since my husband is the head of our household and is not employed by Government.

You might also be interested in the fact that it required 6 hours of after-hours work on our part to hunt up all the information called for and prepare the report. Since the extent of our assets is our private

business, it was necessary that I type the material myself, an added chore since I am not a typist.

Our assets have been derived, in the main, from laying aside a portion of our earnings. At our ages (64 and 58) we would be far less deserving of respect had we not made the prudent provisions for our retirement which our assets and the income they earn represent. Yet this reporting requirement carries with it the implication that to have "clean hands" it would be best to have no assets or outside, unearned income when you work for the Federal Government.

For your information I am a GS–15, earning $19,415. * * *

Thank you for speaking out for the continually maligned civil servant.

Sincerely yours,

———, ———.

DEAR SENATOR ERVIN: I am a GS–12 career employee with over 15 years service.

The highest moral and ethical conduct has been my goal in each of my positions of employment and I have found this to be true of a vast majority of my fellow workers. It may be true a few people do put material gain ahead of their ethics but generally these people are in the higher echelons of office where their influence is much greater.

Our office has recently directed each employee from file clerk to the heads of sections to file a "Statement of Financial Interest." As our office has no programs individuals could have a financial interest in and especially no connections with FHA I feel it is no one's business but my own what real estate I own. I do not have a FHA mortgage or any other real property and have no outside employment, hence have nothing to hide by filing a blank form. Few Government workers can afford much real property. The principle of reporting to "Big Brother" in every phase of your private life to me is very degrading, highly unethical and very unquestionable as to its effectiveness. If I could and did use my position in some way to make a profit I would be stupid to report it on an agency inquiry form. What makes officials think reporting will do away with graft?

When the directive came out many man-hours of productive work were lost in discussions and griping. Daily since that date at some time during the day someone brings up the subject. The supervisors filed their reports as "good" examples but even they objected to this inquiry.

No single thing was ever asked of Government employees that caused such a decline in their morale. We desperately need a "bill of rights" to protect ourselves from any further invasion of our private lives.

Fifteen years ago I committed myself to Government service because: (a) I felt an obligation to the Government due to my education under the GI bill, (b) I could obtain freedom from pressures of unions, (c) I could obtain freedom from invasion of my private life, and (d) I would be given the opportunity to advance based solely on my professional ability and not on personal politics. At this point I certainly regret my decision to make the Government my career.

Sincerely,

———, ———.

DEAR SENATOR: I write to beg your support of a "bill of rights" to protect Federal employees from official snooping which was introduced by Senator Ervin of North Carolina.

I am a veteran of two wars and have orders to a third war as a ready reservist. And I know why I serve in these wars: that is to prevent the forces of tyranny from invading America.

Now, as a Federal employee I must fill out a questionnaire giving details of my financial status. This is required if I am to continue working. I know that this information can be made available to every official in Washington, including those who want to regulate specific details of my life.

Now I am no longer a free American. For example, I can no longer buy stock of a foreign company because that country may be in disfavor with officials of the right or left. And I cannot "own part of America" by buying common stocks until an "approved list" is published by my superiors.

I can never borrow money because an agent may decide that debt makes me susceptible to bribery by agents of an enemy power. Nor do I dare own property lest some official may decide I should sell or rent to a person or group not of my choosing.

In short, I am no longer free to plan my own financial program for the future security of my family. In 1 day I was robbed of the freedom for which I fought two wars. This is a sickening feeling, you may be sure.

It seems plain that a deep, moral issue is involved here that concerns every citizen. If this thing is allowed to continue, tomorrow or next year every citizen may come under the inquisition. The dossier on every citizen will be on file for the use of any person or group having enough overt or covert power to gain access to them.

Sincerely,

———, ———.

On August 1966, Federal employees who were retired from the armed services were told to complete and return within 7 days, with their social security numbers, a 15-page questionnaire, asking, among other things:

> How much did you earn in 1965 in wages, salary, commissions, or tips from all jobs?
>
> How much did you earn in 1965 in profits or fees from working in your own business, professional practice, partnership, or farm?
>
> How much did you receive in 1965 from social security, pensions (nonmilitary) rent (minus expenses), interests or dividends, unemployment insurance, welfare payments, or from any other source not already entered?
>
> How much did other members of your family earn in 1965 in wages, salary, commissions or tips? (Before any deductions.) (For this question, a family consists of two or more persons in the same household who are related to each other by blood, marriage, or adoption.) If the exact amount is not known, give your best estimate.
>
> How much did other members of your family earn in 1965 in profits or fees from working in their own business, professional practices, partnership, or farm?

How much did any other member of your family receive in 1965 from social security, pensions, rent (minus expenses), interest or dividends, unemployment insurance, welfare payments; or from any other source not already entered?

RIGHT TO COUNSEL

Section 1(k) of the bill guarantees to Federal workers the opportunity of asking the presence of legal counsel, of a friend or other person when undergoing an official interrogation or investigation that could lead to the loss of their jobs or to disciplinary action.

The merits of this clause are manifold; not least of which is that uniformity and order it will bring to the present crazy quilt practices of the various agencies concerning the right to counsel for employees facing disciplinary investigations or possible loss of security clearances tantamount to loss of employment. The Civil Service Commission regulations are silent on this critical issue. In the absence of any Commission initiative or standard, therefore, the employing agencies are pursuing widely disparate practices. To judge from the questionnaires and other evidence before the subcommittee, a few agencies appear to afford a legitimate right to counsel, probably many more do not, and still others prescribe a "right" on paper but hedge it in such a fashion as to discourage its exercise. Some apparently do not set any regulatory standard, but handle the problem on an ad hoc basis.

On a matter as critical as this, such a pointless diversity of practice is poor policy. So far as job-protection rights are concerned, all Federal employees should be equal.

A second anomaly in the present state of affairs derives from recent developments in the law of the sixth amendment by the Supreme Court. In view of the decisions of *Miranda* v. *Arizona*, 384 U.S. 436 and *Escobedo* v. *Illinois*, 378 U.S. 478, it is clear that any person (including Federal employees) who is suspected of a crime is absolutely entitled to counsel before being subjected to custodial interrogation. Accordingly, some agencies, such as the Internal Revenue Service, acknowledge an unqualified right to counsel for an employee suspected of crime but decline to do the same for coworkers threatened with the loss of their livelihoods for noncriminal reasons. In the subcommittee's view, this discrimination in favor of the criminal suspect is both bad personnel policy as well as bad law. It would be corrected by this section of the bill.

The ultimate justification for the "right-to-counsel" clause, however, is the Constitution itself. There is no longer any serious doubt that Federal employees are entitled to due process of law as an incident of their employment relation. Once, of course, the courts felt otherwise, holding that absent explicit statutory limitation, the power of the executive to deal with employees was virtually unfettered.

The doctrinal underpinning of this rule was the 19th-century notion that the employment relation is not tangible "property." Both the rule and its underpinning have now been reexamined. The Supreme Court in recent years has emphasized the necessity of providing procedural due process where a man is deprived of his job or livelihood by governmental action.

While the courts have as yet had no occasion to articulate a specific right to counsel in the employment relationship, there can obviously be no doubt that the right to counsel is of such a fundamental character that it is among the essential ingredients of due process. What is at stake for an employee in a discharge proceeding—often including personal humiliation, obloquy and penury—is just as serious as that involved in a criminal trial. This is not to suggest that all the incidents of our civilized standard of a fair trial can or should be imported into Federal discharge proceedings. But if we are to have fair play for Federal employees, the right of counsel is a sine qua non. It is of a piece with the highest traditions, the fairest laws, and the soundest policy that this country has produced. And, in the judgment of this subcommittee, the clear affirmation of this basic right is very long overdue.

The need for such protection was confirmed at the hearings by all representatives of Government employee organizations and unions. The president of the National Association of Letter Carriers testified:

> It is a practice in the postal inspection service, when an employee is called in for questioning by the inspectors on a strictly postal matter that does not involve a felony, to deny the right of counsel. The inspectors interrogate the employee at length and, at the completion of the interrogation, one of the inspectors writes out a statement and pressures the employee to sign it before he leaves the room. We have frequently asked the postal inspection service to permit these employees to have counsel present at the time of the interrogation. The right for such counsel has been denied in all except a few cases. If the employee is charged with a felony, then, of course, the law takes over and the right for counsel is clearly established but in other investigations and interrogations no counsel is permitted.

Several agencies contend that right to counsel is now granted in formal adverse action proceedings and that appeals procedures make this section unnecessary for informal questioning. Testimony and complaints from employees indicate that this machinery does not effectively secure the opportunity of the employee to defend himself early enough in the investigation to allow a meaningful defense.

The predicament of postal employees as described at the hearings reflects the situation in other agencies as reported in many individual cases sent to the subcommittee. While it is undoubtedly true that in some simple questioning, counsel may not be necessary, in many matters where interrogation will result in disciplinary action, failure to have counsel at the first level reacts against the employee all the way up through the appeal and review. In the case of a postal employee, the subcommittee was told—

> The first level is at the working foreman's level. He is the author of the charges; then the case proceeds to the postmaster, who appointed the foreman and, if the individual is found guilty of the charge at the first level, it is almost inevitable that this position will be supported on the second

level. The third level is the regional level, and the policy there is usually that of supporting the local postmaster. A disinterested party is never reached. The fourth level is the Appeals Board, composed of officials appointed by the Postmaster General. In some cases, the region will overrule the postmaster, but certainly the individual does not have what one could style an impartial appeals procedure.

Employees charged with no crime have been subjected to intensive interrogations by Defense Department investigators who ask intimate questions, make sweeping allegations, and threaten dire consequences unless consent is given to polygraph tests. Employees have been ordered to confess orally or to write and sign statements. Such interviews have been conducted after denial of the employee's request for presence of supervisor, counsel, or friend, and in several instances the interrogations have resulted in revocation of a security clearance, or denial of access to classified information by transfer or reassignment, with the resulting loss of promotion opportunities.

Witnesses testified that employees have no recourse against the consequences of formal charges based on information and statements acquired during a preliminary investigation. This renders meaningless the distinction urged by the Civil Service Commission between formal and informal proceedings.

EXCEPTIONS

The act under section 9, does not apply to the Federal Bureau of Investigation. Furthermore, section 6 provides that nothing in the act will prohibit an official of the Central Intelligence Agency and the National Security Agency from requesting any employee or applicant to take a polygraph test or a psychological test, or to provide a personal financial statement designed to elicit the personal information protected under subsections 1 (e), (f), (i), and (j). In such cases, the Director of the agency or his designee must make a personal finding with regard to each individual to be tested or examined that such test or information is required to protect the national security.

An exception to the right-to-counsel section has been provided to limit this right for employees in the Central Intelligence Agency and the National Security Agency to a person who serves in the same agency or a counsel cleared by the agency for access to the information involved. Obviously, it is expected that the employee's right to be accompanied by the person of his choice will not be denied unless that person's access to the information for the purpose of the case is clearly inconsistent with the national security. Other language recognizes problems unique to these two agencies. For instance, section 7 requires exhaustion of remedies by employees of the Central Intelligence Agency and the National Security Agency and states that the act does not affect whatever existing statutory authority these agencies now possess to terminate employment. Section 8 is designed to assure that nothing in the act is construed to affect negatively any existing statutory or executive authority of the Directors of the Central Intelligence Agency and National Security Agency to protect their information in cases involving their employees. Consequently, procedures commended to the subcommitte by the Director of the Central Intelli-

gence Agency are spelled out for asserting that authority in certain proceedings arising under the act. Other committee amendments to S. 1035, as detailed earlier, were adopted to meet adminstrative requirements of the Federal security program and the intelligence community as well as the management needs of the executive branch.

ENFORCEMENT

Enforcement of the rights guaranteed in sections 1 and 2 of the bill is lodged in the administrative and civil remedies and sanctions of sections 3, 4, and 5. Crucial to enforcement of the act is the creation of an independent Board on Employee Rights to determine the need for disciplinary action against civilian and military offenders under the act and to provide relief from violations.

Testimony at the hearings as well as investigation of complaints have demonstrated that in the area of employee rights, a right is only as secure as its enforcement. There is overwhelming evidence that employees have heretofore frequently lacked appropriate remedies either in the courts or the Civil Service Commission for pursuing rights which belong to them as citizens.

Under the remedies afforded by sections 3, 4, and 5 of the bill, an employee who believes his rights are violated under the act has several courses of action:

(1) He may pursue a remedy through the agency procedures established to enforce the act, but the fact that he does not choose to avail himself of these does not preclude exercise of his right to seek other remedies.

(2) He may register his complaint with the Board on Employee Rights and obtain a hearing. If he loses there, he may appeal to the district court, which has the power to examine the record as a whole and to affirm, modify, or set aside any determination or order, or to require the Board to take any action it was authorized to take under the act.

(3) He may, instead of going directly to the Board, institute a civil action in Federal district court to prevent the threatened violation, or obtain complete redress against the consequences of the violation.

He does not need to exhaust any administrative remedies but if he elects to pursue his civil remedies in the court under section 4, he may not seek redress through the Board. Similarly, if he initiates action before the Board under section 5, he may not also seek relief from the court under section 4.

The bill does not affect any authority, right or privilege accorded under Executive Order 11491 governing employee-management cooperation in the Federal service. To the extent that there is any overlapping of subject matter, the bill simply provides an additional remedy.

THE BOARD ON EMPLOYEES' RIGHTS

As a result of hearings on S. 3779, the section creating a Board on Employees' Rights was added to the bill for introduction as S. 1035.

Employees have complained that administrative grievance pro-

cedures have often proved ineffective because they are cumbersome, time-consuming, and weighted on the side of management. Not only do those who break the rules go unpunished many times, but the fearful tenor of letters and telephone calls from throughout the country indicate that employees fear reprisals for noncompliance with improper requests or for filing of complaints and grievances. Oral and written directives of warning to this effect have been verified by the subcommittee. Section 1(e) of the bill, therefore, prevents reprisals for exercise of rights granted under the act and in such event accords the individual cause for complaint before the Board or the court.

Concerning the original bill in the 89th Congress, which did not provide for a board, representatives of the 14th department of the American Federation of Government Employees commented that the remedies are the most important aspects of such a bill because "unless due process procedures are explicitly provided, the remaining provisions of the bill may be easily ignored or circumvented by Federal personnel management. As a matter of fact, we believe, the reason employees' rights have been eroded so rapidly and so devastatingly in the last few years is the absence of efficient, expeditious, uniform, and legislatively well defined procedures of due process in the executive departments of the Federal Government."

An independent and nonpartisan Board is assured by congressional participation in its selection and by the fact that no member is to be a government employee. Provision is made for congressional monitoring through detailed reports.

Senator Ervin explained the function of the Board established by section 5 as follows:

> The bill sets up a new independent Federal agency with authority to receive complaints and make rulings on complaints—complaints of individual employees or unions representing employees. This independent agency, which would not be subject in any way to the executive branch of the Government, would be authorized to make rulings on these matters in the first instance. It would make a ruling on action in a particular agency or department that is an alleged violation of the provisions of the bill, with authority either on the part of the agency or the part of the individual or on the part of the union to take an appeal from the ruling of this independent agency to the Federal court for judicial review.

Throughout its study the subcommittee found that a major area of concern is the tendency in the review process in the courts or agencies to do no more than examine the lawfulness of the action or decision about which the employee has complained. For purposes of enforcing the act, sections 3, 4 and 5 assure adequate machinery for processing complaints and for prompt and impartial determination of the fairness and constitutionality of general policies and practices initiated at the highest agency levels or by the Civil Service Commission or by Executive order.

Finding no effective recourse against administrative actions and policies which they believed unfair or in violation of their rights, individual employees and their families turned to Congress for redress. Opening the hearings on invasions of privacy, Senator Ervin stated:

> Never in the history of the Subcommittee on Constitutional Rights have we been so overwhelmed with personal complaints, phone calls, letters, telegrams, and office visits. In all of our investigations I have never seen anything to equal the outrage and indignation from Government employees, their families, and their friends. It is obvious that appropriate remedies are not to be found in the executive branch.
>
> The complaints of privacy invasions have multiplied so rapidly of late that it is beyond the resources of Congress and its staff to repel effectively each individual official encroachment. Each new program brings a new wave of protest.

Prof. Alan Westin, director of the Science and Law Committee of the Bar Association of the city of New York, testified that these complaints "have been triggered by the fact that we do not yet have the kind of executive branch mechanism by which employees can lodge their sense of discomfort with personnel practices in the Federal Government and feel that they will get a fair hearing, that they will secure what could be called 'employment due process.'"

To meet this problem, Professor Westin proposed an independent board subject to judicial review, and with enforcement power over a broad statutory standard governing all invasion of privacy. Although it is continuing to study this proposal, the subcommittee has temporarily rejected this approacch in the interest of achieving immediate enforcement of the act and providing administrative remedies for its violation. For this reason it supports the creation of a limited Board on Employees' Rights.

Perhaps one of the most important sections of the bill, if not the most important section, according to the United Federation of Postal Clerks, is the provision establishing the Board. The subcommittee was told—

> It would appear absolutely essential that any final legislation enacted into law must necessarily include such a provision. We can offer no suggestion for improvement of this section. As presently constituted the section is easily understood; and the most excellent and inclusive definition of the proposed "Board on Employees' Rights" which could possibly be enacted into law. It defines the right of employees to challenge violations of the proposed act; defines the procedures involved, as well as the authority of the Board, penalties for violation of the act, as well as establishing the right of judicial review for an aggrieved party, and finally provides for congressional review, and in effect, an annual audit by the Congress of all complaints, decisions, orders, and other related information resulting from activities and operations of the proposed act.

Sanctions

The need for sanctions against offending officials has been evident throughout the subcommittee's investigation of flagrant disregard of basic rights and unpunished flaunting of administrative guidelines and prohibitions. It was for this reason that S. 3779 of the 89th Congress and S. 1035, as introduced, contained criminal penalties for offenders and afforded broad civil remedies and penalties.

Reporting on the experiences of the American Civil Liberties Union in such employee cases, Lawrence Speiser testified:

> In filing complaints with agencies including the Civil Service Commission, the Army and the Navy, as I have during the period of time I have worked here in Washington, I have never been informed of any disciplinary action taken against any investigator for asking improper questions, for engaging in improper investigative techniques, for barring counsel when a person had a right to have counsel, or for a violation of any number of things that you have in this bill. Maybe some was taken, but I certainly couldn't get that information out of the agencies, after making the complaints. I would suggest that the bill also encompass provision for disciplinary action that would be taken against Federal employees who violate any of these rights that you have set out in the bill.

Other witnesses also pointed to the need for the disciplinary measures afforded by the powers of an independent Board to determine the need for corrective action and punishment, and felt they would be more effective than criminal penalties.

In view of the difficulty of filing criminal charges and obtaining prosecution and conviction of executive branch officials which might render the criminal enforcement provision meaningless for employees, the criminal penalties were deleted and a Board on Employee Rights incorporated into the scheme of remedies and sanctions in the bill.[1]

Although the Civil Service Commission and the executive agencies have advocated placing such administrative remedies within the civil service grievance and appeals system, the subcommittee believes that the key to effective enforcement of the unique rights recognized by this act lies in the employee's recourse to an independent body.

"The theory of our Government," Professor Westin testified, "is that there should be somewhere within the executive branch where this kind of malpractice is corrected and that good administration ought to provide for control of supervision or other practices that are not proper. But the sheer size of the Federal Establishment, the ambiguity of the relationship of the Civil Service Commission to employees, and the many different interests that the Civil Service Commission has to bear in its role in the Federal Government, suggest that it is not an effective instrument for this kind of complaint procedure."

SECTION-BY-SECTION ANALYSIS

SECTION 1

Section 1(a) makes it unlawful for a Federal official of any department or agency to require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency or any person seeking employment to disclose his race, religion, or national origin, or the race, religion, or national origin of any of his forebears.

This section does not prohibit inquiry concerning citizenship of such individual if his citizenship is a statutory condition of his obtaining or

[1] In the 89th Congress, S. 1035.

retaining his employment. Nor does it preclude inquiry of the individual concerning his national origin or citizenship or that of his forebears when such inquiry is thought necessary or advisable in order to determine suitability for assignment to activities or undertakings related to national security within the United States or to activities or undertakings of any nature outside the United States.

This provision is directed at any practice which places the employee or applicant under compulsion to reveal such information as a condition of the employment relation. It is intended to implement the concept underlying the Federal merit system by which a person's race, religion, or national origin have no bearing on his right to be considered for Federal employment or on his right to retain a Federal position. This prohibition does not limit the existing authority or the executive branch to acquire such information by means other than self-disclosure.

Section 1(b) makes it unlawful for any officer of any executive department or executive agency of the U.S. Government, or for any person acting or purporting to act under this authority, to state, intimate, or to attempt to state or intimate, to any civilian employee of the United States serving in the department or agency that any notice will be taken of his attendance or lack of attendance at any assemblage, discussion, or lecture held or called by any officer of the executive branch of the U.S. Government, or by any person acting or purporting to act under his authority, or by any outside parties or organizations to advise, instruct, or indoctrinate any civilian employee of the United States serving in the department or agency in respect to any matter or subject other than (1) the performance of official duties to which he is or may be assigned in the department or agency, or (2) the development of skills, knowledge, or abilities which qualify him for the performance of such duties.

Nothing contained in this section is to be construed to prohibit taking notice of the participation of a civilian employee in the activities of any professional group or association.

This provision is designed to protect any employee from compulsion to attend meetings, discussions, and lectures on political, social, and economic subjects unrelated to his duties. It prevents Government officials from using the employment relationship to attempt to influence employee thoughts, attitudes, and actions on subjects which may be of concern to them as private citizens. In particular, this language is directed at practices and policies which in effect require attendance at such functions, including official lists of those attending or not attending; its purpose is to prohibit threat, direct or implied, written or oral, of official retaliation for nonattendance.

This section does not affect existing authority for providing information designed to promote the health and safety of employees. Nor does it affect existing authority to call meetings for the purpose of publicizing and giving notice to activities or service, sponsored by the department or agency, or campaigns such as charitable fund campaigns and savings bond drives.

Section 1(c) makes it unlawful for any officer of any executive department or agency, or for any person acting or purporting to act under his authority, to require or request or to attempt to require or

request any civilian employee serving in the department or agency to participate in any way in any activities or undertakings unless they are related to the performance of official duties to which he is or may be assigned in the department or agency or to the development of skills, knowledge, or abilities which qualify him for the performance of such duties.

This section is directed against official practices, requests, or orders that an employee take part in any civic function, political program, or community endeavor, or other activity which he might enjoy as a private citizen, but which is unrelated to his employment. It does not affect any existing authority to use appropriate techniques for publicizing existence of community programs such as blood-donation drives, or agency programs, benefits or services, and for affording opportunity for employee participation if he desires.

Section 1(d) makes it unlawful for any officer of any executive department or agency, or for any person acting under his authority to require or request or attempt to require or request, any civilian employee serving in the department or agency to make any report of his activities or undertakings unless they are related to the performance of official duties or to the development of skills, knowledge, or abilities which qualify him for the performance of such duties, or (2) unless there is reason to believe that the employee is engaged in outside activities or employment in conflict with his official duties.

This section is a minimum guarantee of the freedom of an employee to participate or not to participate in any endeavor or activity in his private life as a citizen, free of compulsion to report to supervisors his action or his inaction, his involvement or his noninvolvement. This section is to assure that in his private thoughts, actions, and activities he is free of intimidation or inhibition as a result of the employment relation.

The exceptions to the prohibition are not legislative mandates to require such information in those circumstances, but merely provide an area of executive discretion for reasonable management purposes and for observance and enforcement of existing laws governing employee conduct and conflicts of interest.

Section 1(e) makes it unlawful for any officer of any executive department or agency, or any person acting under his authority, to require or request any civilian employee serving in the department or agency, or any person applying for employment as a civilian employee to submit to any interrogation or examination or to take any psychological test designed to elicit from him any information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

In accordance with an amendment made after hearings on S. 3779, a proviso is included to assure that nothing contained in this section shall be construed to prevent a physician from eliciting such information or authorizing such test in the diagnosis or treatment of any civilian employee or applicant where he feels the information is necessary to enable him to determine whether or not the individual is suffering from mental illness. The bill as introduced limited this inquiry to psychiatrists, but an amendment extended it to physicians,

since the subcommittee was told that when no psychiatrist is available, it may be necessary for a general physician to obtain this information in determining the presence of mental illness and the need for further treatment.

This medical determination is to be made in individual cases and not pursuant to general practice or regulation governing the examination of employees or applicants according to grade, agency, or duties.

Under an amendment to the bill, this language is not to be construed to prohibit an official from advising an employee or applicant of a specific charge of sexual misconduct made against that person and affording him an opportunity to refute the charge. While providing no authority to request or demand such information, the section does not prevent an official who has received charges of misconduct which might have a detrimental effect on the person's employment from obtaining a clarification of the matter if the employee wishes to provide it.

This section would not prohibit all personality tests but merely those questions on the tests which inquire into the three areas in which citizens have a right to keep their thoughts to themselves.

It raises the criterion for requiring such personal information from the general "fitness for duty" test to the need for diagnosing or treating mental illness. The second proviso is designed to prohibit mass-testing programs. The language of this section provides guidelines for the various personnel and medical specialists whose practices and determinations may invade employee's personal privacy and thereby affect the individual's employment prospects or opportunities for advancement.

An amendment in section 6 provided an exception to this prohibition in the case of the use of such psychological tests by the Central Intelligence Agency and the National Security Agency, only if the Director of the agency or his designee makes a personal finding that the information is necessary to protect the national security.

Section 1(f) makes it unlawful for any officer of any executive department or agency or any person acting under his authority, to require or request or attempt to require or request any civilian employee or any applicant for employment to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices or concerning his attitude or conduct with respect to sexual matters. While this section does not eliminate entirely the use of so-called lie detectors in Government, it assures that where such devices are used, officials may not inquire into matters which are of a personal nature.

As with psychological testing, the Central Intelligence Agency and the National Security Agency, under section 6, are not prohibited from acquiring such information by polygraph, provided certain conditions are met.

Section 1(g) makes it illegal for an official to require or request an employee under his management to support the nomination or election of anyone to public office through personal endeavor, financial contribution, or any other thing of value. An employee may not be required or requested to attend any meeting held to promote or support the activities or undertakings of any political party in the United States.

The purpose of this section is to assure that the employee is free from any job-related pressures to conform his thoughts and attitudes and actions in political matters unrelated to his job to those of his supervisors. With respect to his superiors, it protects him in the privacy of his contribution or lack of contribution to the civic affairs and political life of his community, State and Nation. In particular, it protects him from commands or requests of his employer to buy tickets to fundraising functions, or to attend such functions, to compile position papers or research material for political purposes, or make any other contribution which constitutes a political act or which places him in the position of publicly expressing his support or nonsupport of a party or candidate. This section also assures that, although there is no evidence of such activities at present, no Federal agency may in the future improperly involve itself in the undertakings of any political party in the United States, its territories, or possessions.

Section 1(h) makes it illegal for an official to coerce or attempt to coerce any civilian employee in the department or agency to invest his earnings in bonds or other Government obligations or securities, or to make donations to any institution or cause. This section does not prohibit officials from calling meetings or taking any other appropriate action to afford employees the opportunity voluntarily to invest his earnings in bonds or other obligations or voluntarily to make donations to any institution or cause. Appropriate action, in the committee's view, might include publicity and other forms of persuasion short of job-related pressures, threats, intimidation, reprisals of various types, and "blacklists" circulated through the employee's office or agency to publicize his noncompliance.

Section 1(i) makes it illegal for an official to require or request any civilian employee in the department or agency to disclose any items of his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family. Exempted from coverage under this provision is any civilian employee who has authority to make any final determination with respect to the tax or other liability to the United States of any person, corporation, or other legal entity, or with respect to claims which require expenditure of Federal moneys. Section 6 provides certain exemptions for two security agencies.

Neither the Department of the Treasury nor any other executive department or agency is prohibited under this section from requiring any civilian employee to make such reports as may be necessary or appropriate for the determination of his liability for taxes, tariffs, custom duties, or other obligations imposed by law. This proviso is to assure that Federal employees may be subject to any reporting or disclosure requirements demanded by any law applicable to all persons in certain circumstances.

Section 1(j) makes it illegal to require or request any civilian employee exempted from application of section 3(i) under the first proviso of that section, to disclose any items of his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family or household other than specific items tending to indicate a conflict of interest

in respect to the performance of any of the official duties to which he is or may be assigned.

This section is designed to abolish and prohibit broad general inquiries which employees have likened to "fishing expeditions" and to confine any disclosure requirements imposed on an employee to reasonable inquiries about job-related financial interests. This does not preclude, therefore, questioning in individual cases where there is reason to believe the employee has a conflict of interest with his official duties.

Section 1(k) makes it unlawful for a Federal official of any department or agency to require or request, or attempt to require or request, a civilian employee who is under investigation for misconduct, to submit to interrogation which could lead to disciplinary action without the presence of counsel or other person of his choice, if he wishes.

This section is intended to rectify a longstanding denial of due process by which agency investigators and other officials prohibit or discourage presence of counsel or a friend. This provision is directed at any interrogation which could lead to loss of job, pay, security clearance, or denial of promotion rights.

This right insures to the employee at the inception of the investigation, and the section does not require that the employee be accused formally of any wrongdoing before he may request presence of counsel or friend. The section does not require the agency or department to furnish counsel.

A committee amendment to S. 782 adds a proviso that a civilian employee serving in the Central Intelligence Agency or the National Security Agency may be accompanied only by a person of his choice who serves in the agency in which the employee serves, or by counsel who has been approved by the agency for access to the information involved.

Section 1(l) makes it unlawful for a Federal official of any department or agency to discharge, discipline, demote, deny promotion, relocate, reassign, or otherwise impair existing terms or conditions of employment of any employee, or threaten to commit any such acts, because the employee has refused or failed to comply with any action made unlawful by this act or exercised any right granted by the act.

This section prohibits discrimination against any employee because he refuses to comply with an illegal order as defined by this act or takes advantage of a legal right embodied in the act.

SECTION 2

Section 2(a) makes it unlawful for any officer of the U.S. Civil Service Commission or any person acting or purporting to act under his authority to require or request, or attempt to require or request, any executive department or any executive agency of the U.S. Government, or any officer or employee serving in such department or agency, to violate any of the provisions of section 1 of this act.

Specifically, this section is intended to ensure that the Civil Service Commission, acting as the coordinating policymaking body in the area of Federal civilian employment shall be subject to the same strictures as the individual departments or agencies.

Section 2(b) makes it unlawful for any officer of the U.S. Civil Service Commission, or any person acting or purporting to act under his authority, to require or request, or attempt to require or request, any person seeking to establish civil service status or eligibility for civilian employment, or any person applying for employment, or any civilian employee of the United States serving in any department or agency, to submit to any interrogation or examination or to take any psychological test which is designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

This section is intended to assure that the Civil Service Commission shall be subject to the same prohibitions to which departments and agencies are subject in sections 1 (e) and (f). The provisos contained in section 1(e) are restated here to assure that nothing in this section is to be construed to prohibit a physician from acquiring such data to determine mental illness, or an official from informing an individual of a specific charge of sexual misconduct and affording him an opportunity to refute the charge.

Section 2(c) makes it unlawful for any officer of the U.S. Civil Service Commission to require or request any person seeking to establish civil service status or eligibility for employment, or any person applying for employment in the executive branch of the U.S. Government, or any civilian employee serving in any department or agency to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

This section applies the provisions of section 1(f) to the Civil Service Commission in instances where it has authority over agency personnel practices or in cases in which its officials request information from the applicant or employee.

SECTION 3

This section applies the act to military supervisors by making violations of the act also violations of the Uniform Code of Military Justice.

SECTION 4

Section 4 provides civil remedies for violation of the act by granting an applicant or employee the right to bring a civil action in the Federal district court for a court order to halt the violation, or to obtain complete redress against the consequences of the violation. The action may be brought in his own behalf or in behalf of himself and others similarly situated, and the action may be filed against the offending officer or person in the Federal District court for the district in which the violation occurs or is threatened, or in the district in which the offending officer or person is found, or in the District Court for the District of Columbia.

The court hearing the case shall have jurisdiction to adjudicate the civil action without regard to the actuality or amount of pecuniary

injury done or threatened. Moreover, the suit may be maintained without regard to whether or not the aggrieved party has exhausted available administrative remedies. If the individual complainant has pursued his relief through administrative remedies established for enforcement of the act and has obtained complete protection against threatened violations or complete redress for violations, this relief may be pleaded in bar of the suit. The court is empowered to provide whatever broad equitable and legal relief it may deem necessary to afford full protection to the aggrieved party; such relief may include restraining orders, interlocutory injunctions, permanent injunctions, mandatory injunctions, or such other judgments or decrees as may be necessary under the circumstances.

Another provision of section 4 would permit an aggrieved person to give written consent to any employee organization to bring a civil action on his behalf, or to intervene in such action. "Employee organizations" as used in this section includes any brotherhood, council, federation, organization, union, or professional association made up in whole or in part of Federal civilian employees, and which deals with departments, agencies, commissions, and independent agencies regarding employee matters.

A committee amendment provides that the Attorney General shall defend officers or persons who acted pursuant to an order, regulation, or directive, or who, in his opinion, did not willfully violate the provisions of the act.

SECTION 5

Section 5 establishes an independent Board on Employees' Rights, to provide employees with an alternative means of obtaining administrative relief from violations of the act, short of recourse to the judicial system.

Section 5(a) provides for a Board composed of three members, appointed by the President with the consent of the Senate. No member shall be an employee of the U.S. Government and no more than two members may be of the same political party. The President shall designate one member as Chairman.

Section 5(b) defines the term of office for members of the Board, providing that one member of the initial Board shall serve for 5 years, one for 3 years, and one for 1 year from the date of enactment; any member appointed to fill a vacancy in one of these terms shall be appointed for the remainder of the term. Thereafter, each member shall be appointed for 5 years.

Section 5(c) establishes the compensation for Board members at $75 for each day spent working in the work of the Board, plus actual travel expenses and per diem in lieu of subsistence expenses when away from their usual places of residence.

Section 5(d) provides that two members of the Board shall constitute a quorum for the transaction of business.

Section 5(e) provides that the Board may appoint and fix the compensation of necessary employees, and make such expenditures necessary to carry out the functions of the Board.

Section 5(f) authorizes the Board to make necessary rules and regulations to carry out its functions.

Section 5(g) provides that the Board shall have the authority and duty to receive and investigate written complaints from or on behalf of any person claiming to be affected or aggrieved by any violation or threatened violation of this act, and to conduct a hearing on each such complaint. Moreover, within 10 days after the receipt of such a complaint, the Board must furnish notice of time, place, and nature of the hearing to all interested parties, and within 30 days after concluding the hearing, it must render its final decision regarding any complaint.

Section 5(h) provides that officers or representatives of any employee organization in any degree concerned with employment of the category in which the violation or threat occurs, shall be given an opportunity to participate in the hearing through submission of written data, views, or arguments. In the discretion of the Board they are to be afforded an opportunity for oral presentation. This section further provides that Government employees called upon by any party or by any Federal employee organization to participate in any phase of any administrative or judicial proceeding under this section shall be free to do so without incurring travel cost or loss in leave or pay. They shall be free from restraint, coercion, interference, intimidation, or reprisal in or because of their participation. Any periods of time spent by Government employees during such proceedings shall be held to be Federal employment for all purposes.

Section 5(i) applies to the Board hearings the provisions of the Administrative Procedure Act relating to notice and conduct of hearings insofar as consistent with the purpose of this section.

Section 5(j) requires the Board, if it determines after a hearing that this act has not been violated, to state such determination and notify all interested parties of the findings. This determination shall constitute a final decision of the Board for purposes of judicial review.

Section 5(k) specifies the action to be taken by the Board if, after a hearing, it determines that any violation of this act has been committed or threatened. In such case, the Board shall immediately issue and cause to be served on the offending officer or employee an order requiring him to cease and desist from the unlawful practice or act. The Board is to endeavor to eliminate the unlawful act or practice by informal methods of conference, conciliation, and persuasion.

Within its discretion, the Board may, in the case of a first offense, issue an official reprimand against the offending officer or employee, or order the employee suspended from his position without pay for a period not exceeding 15 days. In the case of a second or subsequent offense, the Board may order, the offending officer or employee suspended without pay for a period not exceeding 30 days, or may order his removal from office.

Officers appointed by the President, by and with the advice and consent of the Senate, are specifically excluded from the application of these disciplinary measures; but the section provides that, in the case of a violation of this act by such individuals, the Board may transmit a report concerning such violation to the President and the Congress.

Section 5(l) provides for Board action when any officer of the Armed Forces of the United States or any person acting under his authority violates the act. In such event, the Board shall (1) submit a report to

the President, the Congress, and to the Secretary of the military department concerned, (2) endeavor to eliminate any unlawful act or practice through informal methods of conference, conciliation, and persuasion, and (3) refer its determination and the record in the case to any person authorized to convene general courts-martial under section 822 (article 22) of title 10, United States Code. When this determination and report is received, the person designated shall immediately dispose of the matter under the provisions of chapter 47 of title 10 of the United States Code.

Section 5(m) provides that when any party disagrees with an order or final determination of the Board, he may institute a civil action for judicial review in the Federal district court for the district wherein the violation or threatened violation occurred, or in the District Court for the District of Columbia.

The court has jurisdiction to (1) affirm, modify, or set aside any determination or order made by the Board, or (2) require the Board to make any determination or order which it is authorized to make under section 5(k) but which it has refused to make. In considering the record as a whole, the court is to set aside any finding, conclusion, determination, or order of the Board unsupported by substantial evidence.

The type of review envisioned here is similar to that obtained under the Administrative Procedure Act in such cases but this section affords a somewhat enlarged scope for consideration of the case than is now generally accorded on appeal of employee cases. The court here has more discretion for action on its own initiative. To the extent that they are consistent with this section, the provisions for judicial review in title 5 of the United States Code would apply.

Section 5(n) provides for congressional review by directing the Board to submit to the Senate and to the House of Representatives an annual report which must include a statement concerning the nature of all complaints filed with it, the determinations and orders resulting from hearings, and the names of all officers or employees against whom any penalties have been imposed under this section.

Section 5(o) provides an appropriation of $100,000 for the Board on Employee Rights.

SECTION 6

Section 6 provides that nothing in the act shall be construed to prohibit an officer of the Central Intelligence Agency or of the National Security Agency, under specific conditions, from requesting an applicant or employee to submit a personal financial statement of the type defined in subsection 1 (i) and (j) or to take any polygraph or psychological test designed to elicit the personal information protected under subsection 1(e) or 1(f).

In these agencies, such information may be acquired from the employee or applicant by such methods only if the Director of the agency or his designee makes a personal finding with regard to each individual that such test or information is required to protect the national security.

SECTION 7

Section 7 requires, in effect, that employees of the Central Intelligence Agency and the National Security Agency exhaust their admin-

istrative remedies before invoking the provisions of section 4 (the Board on Employee Rights) or section 5 (the Federal court action). An employee, his representative, or any organization acting in his behalf, must first submit a written complaint to the agency and afford it 120 days to prevent the threatened violation or to redress the actual violation. A proviso states that nothing in the act affects any existing legal authority of the Central Intelligence Agency under 50 U.S.C. 403(c) or of the National Security Agency under 50 U.S.C. 833 to terminate employment.

SECTION 8

Section 8 provides that nothing in the act shall be construed to affect in any way authority of the directors of the Central Intelligence Agency or the National Security Agency to protect or withhold information pursuant to statute or Executive order. In cases involving his employees, the personal certification by the Director of the agency that disclosure of any information is inconsistent with the provision of any statute or Executive order is to be conclusive and no such information shall be admissible in evidence in any civil action under section 4 or in any proceeding or civil action under section 5. Nor may such information be receivable in the record of any interrogation of an employee under section 1(k).

SECTION 9

Section 9 provides that the Federal Bureau of Investigation shall be excluded from the provisions of this act.

SECTION 10

Section 10 provides that nothing contained in sections 4 or 5 shall be construed to prevent the establishment of department and agency grievance procedures to enforce this act. The section makes it clear that the existence of such procedures are not to preclude any applicant or employee from pursuing any other available remedies. However, if under the procedures established by an agency, the complainant has obtained complete protection against threatened violations, or complete redress for violations, such relief may be pleaded in bar in the U.S. district court or in proceedings before the Board on Employees' Rights.

Furthermore, an employee may not seek his remedy through both the Board and the court. If he elects to pursue his remedies through the Board under section 5, for instance, he waives his right under section 4 to take his case directly to the district court.

SECTION 11

Section 11 is the standard severability clause.

93D CONGRESS
1ST SESSION

S. 2542

IN THE SENATE OF THE UNITED STATES

OCTOBER 8, 1973

Mr. BAYH introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To protect the constitutional right of privacy of those individuals concerning whom certain records are maintained, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That (a) subchapter II of chapter 5 of title 5, United States Code, is amended by adding immediately after section 552 thereof the following new section:

"§ 552a. Individual records

"(a) Each agency that shall maintain records concerning any individual which may be retrieved by reference to, or are indexed under, the individual's name and which contain

any information obtained from any source other than such individual shall, with respect to such records—

"(1) notify such individual by mail at his last known address that the agency maintains or is about to maintain a record concerning said individual:

"(2) refrain from disclosing the record or any information contained therein to any other agency or to any person not employed by the agency maintaining such record, except with permission of the individual concerned or, in the event said individual cannot be located or communicated with after reasonable effort, with permission from members of the individual's immediate family or guardian, or, only in the event that such individual, members of the individual's immediate family, and guardian cannot be located or communicated with after reasonable effort, upon good cause for such disclosure: *Provided, however,* That if disclosures of said record is required under section 552 of this chapter or by any other provision of law, the individual concerned shall be notified by mail at his last known address of any such required disclosure;

"(3) maintain an accurate record of the names and positions of all persons inspecting such records and the purposes for which such inspections were made;

"(4) permit any individual to inspect his own record and have copies thereof made at his expense;

"(5) permit any individual to supplement the information contained in his record by the addition of any document or writing containing information such individual deems pertinent to his record, and

"(6) remove erroneous information of any kind.

"(b) Each agency may establish published rules stating the time, place, fees to the extent authorized, and procedure to be followed with respect to making records promptly available to an individual, and otherwise to implement the provisions of this section.

"(c) This section shall not apply to records that are—

"(1) specifically required by Executive order to be kept secret in the interest of the national security;

"(2) investigatory files compiled for law enforcement purposes, except to the extent that such records have been maintained for a longer period than reasonably necessary to commence prosecution or other action or to the extent available by law to a party other than an agency; and

"(3) interagency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.

"(d) The President shall report to Congress before January 30 of each year on an agency-by-agency basis the number of records and the number of investigatory files which were exempted from the application of this section by reasons of clauses (1) and (2) of subsection (d) during the immediately preceding calendar year.

"(e) This section shall not be held or considered to permit the disclosure of the identity of any person who has furnished information contained in any record subject to this section.

"(f) If any provision of this section or the application of such provision to any person or circumstance shall be held invalid, the validity of the remainder of this section and the applicability of such provision to other persons or circumstances shall not be affected thereby.".

(b) The table of sections of subchapter II of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Individual records."

immediately below:

"552. Public information; agency rules; opinions, orders, records, and proceedings.".

SEC. 2. (a) There is established a Board to be known as the Federal Privacy Board (hereinafter referred to as the "Board").

(b) The Board shall consider complaints from any indi-

vidual that one or more of the requirements of section 552(a) of title 5, United States Code, have not been met, with respect to the records specified in such section, by the responsible agency. The Board upon finding that one or more of the requirements have not been met, shall issue a final order directing the agency to comply with such requirement or requirements, and this order shall be binding on the parties to such a dispute.

(c) The Board shall consist of seven members, each serving for a term of two years, four of whom shall constitute a quorum. Three members shall be appointed by the Speaker of the House, three by the President pro tempore of the Senate, and one by the President. No more than two of the members appointed by the Speaker of the House shall be of the same political party. No more than two of the members appointed by the President pro tempore of the Senate shall be of the same political party. The member appointed by the President shall be from the public at large. Any vacancy in the Board shall be filled in the same manner the original appointment was made.

(d) Members of the Board shall be entitled to receive $100 each day during which they are engaged in the performance of the business of the Board, including traveltime, but members who are full-time officers or employees of the

United States shall receive no additional compensation on account of their services as members.

(e) The Chairman of the Board shall be elected by the Board every year, and the Board shall meet not less frequently than bimonthly.

(f) The Board shall appoint and fix the compensation of such personnel as are necessary to the carrying out of its duties.

(g) The Board shall hold hearings in order to make findings upon each complaint, unless there are reasonable grounds to believe that the complaint is frivolous or irrelevant. The Board may examine such evidence as it deems useful, and shall establish such rules and procedures as it determines are most apt to the purposes of this section, including rules insuring the exhaustion of administrative remedies in the appropriate agency.

SEC. 3. (a) Section 2511 (2) of title 18, United States Code, is amended—

(1) by striking out in paragraph (c) "(c) It" and inserting in lieu thereof "(c) (i) Subject to the provisions of clause (iii), it"; and

(2) by striking out in paragraph (d) "(d) It" and inserting in lieu thereof "(ii) Subject to the provisions of clause (iii), it".

(b) Section 2511(2)(c) of such title 18 is further amended by adding at the end thereof the following new clause:

"(iii) It shall not be unlawful under this chapter for a person to intercept a telephone conversation by means of a recording device where such person is a party to the conversation, has given adequate notice to all parties to the conversation that the conversation is being recorded, and uses an automatic tone warning device which automatically produces an audible distant signal that is repeated at regular intervals during the course of the telephone conversation when the recording device is in use. The Federal Communications Commission shall prescribe by regulation the characteristics of an automatic tone warning device that may be used in connection with the authorized interception of telephone conversations.".

SEC. 4. The amendments made by this Act shall become effective on the ninetieth day following the date of enactment of this Act.

[Note. Senator Goldwater did not have any Introductory Remarks in the Record on S. 2810]

93D CONGRESS
1ST SESSION

S. 2810

IN THE SENATE OF THE UNITED STATES

DECEMBER 13, 1973

MR. GOLDWATER introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To protect the constitutional right of privacy of individuals concerning whom identifying numbers or identifiable information is recorded by enacting principles of information practice in furtherance of amendments I, III, IV, V, IX, X, and XIV of the United States Constitution.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. This Act may be cited as the "Right to Privacy Act of 1973".

FINDINGS AND DECLARATION OF PURPOSE

SEC. 2. (a) The Congress finds—

(1) that an individual's personal privacy is directly affected by the kind of disclosure and use made of iden-

tifying numbers and identifiable information about him in a record;

(2) that a record containing information about an individual in identifiable form must be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it;

(3) that any recording, disclosure, and use of identifiying numbers and identifiable personal information by an organization not governed by such procedures must be prohibited as an unfair information practice unless such recording, disclosure, or use is specifically authorized by the data subject or by Federal statute.

(b) The purpose of this Act is to insure safeguards for personal privacy from recordkeeping organizations by adherence to the following principles of information practice:

(1) There must be no personal data recordkeeping systems whose very existence is secret.

(2) There must be a way for an individual to find out what information about him is in a record and how it is used.

(3) There must be a way for an individual to prevent information about him obtained for one purpose

from being used or made available for other purposes without his consent.

(4) There must be a way for an individual to correct or amend a record of identifiable information about him.

(5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

(6) Deviations from these principles should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount interest of society can be clearly demonstrated. No deviation should be permitted except as specifically provided by statute.

DEFINITIONS

SEC. 3. For the purposes of this Act—

(a) The term "automated personal data system" means a collection of records containing personal data that can be associated with identifiable individuals, and that are stored, in whole or in part, in computer-accessible files.

(b) The term "data that can be associated with identifiable individuals" means that by some specific identifica-

tion, such as a name or social security number, or because they include personal characteristics, it is possible to identify an individual with reasonable certainty.

(c) The term "personal data" includes all data that (1) describes anything about an individual, such as identifying characteristics, measurements, test scores; (a) indicates things done by or to an individual, including, but not limited to, records of financial transactions, medical treatment, or other services; or (3) affords a clear basis for inferring personal characteristics or things done by or to an individual, including, but not limited to, the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution.

(d) The term "computer accessible" means recorded on magnetic tape, magnetic disk, magnetic drum, punched card, or optically scannable paper or film.

(e). The term "data system" includes all processing operations, from initial collection of data through all uses of the data, including outputs from the system. Data recorded on questionnaires, or stored in microfilm archives, shall be considered part of a data system, even when the computer-accessible files themselves do not contain identifying information.

(f) The term "organization" means any Federal agency;

the courts of the United States; the government of the District of Columbia; any public or private corporation, partnership, agency, or association which operates an administrative automated personal data system, or a statistical-reporting and research automated personal data system; and which is supported in whole or in part by Federal funds, Federal systems, or federally supported systems, or which directly or indirectly makes use of any means or instruments of transportation or communications in interstate commerce, or of the mails, or which carries or causes to be carried in the mails or interstate commerce, or by any other means or instruments of transportation any personal data; and any organization which maintains a record of individually identifiable personal data which it does not maintain as part of an administrative or as a statistical-reporting and research automated personal data system and which transfers such data to one of the above organizations in interstate commerce.

(g) The term "administrative personal data system" means one that maintains data on individuals for the purpose of affecting them directly as individuals, including, but not limited to, the purpose of making determinations relating to their qualifications, character, rights, opportunities, or benefits.

(h) The term "statistical-reporting or research system"

means one that maintains data about individuals exclusively for statistical reporting or research and is not intended to be used to affect any individual directly.

(i) The term "unfair personal information practice" means a failure to comply with any safeguard requirements of this Act.

(j) The term "data subject" means the individual whose name or identity is added to or maintained on an automated personal data system or a statistical-reporting or research system.

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE PERSONAL DATA SYSTEMS

SEC. 4. (a) GENERAL REQUIREMENTS.—(1) Any organization maintaining a record of individually identifiable personal data, which it does not maintain as part of an administrative automated personal data system, shall make no transfer of any such data to another organization, without the prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an administrative automated personal data system that is not subject to these safeguard requirements.

(2) Any organization maintaining an administrative automated personal data system shall—

(A) identify one person immediately responsible for

the system, and make any other organizational arrangements that are necessary to assure continuing attention to the fulfillment of these safeguard requirements;

(B) take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all these safeguard requirements and all the rules and procedures of the organization designed to assure compliance with them, and the nature of such action shall be supplied upon the reasonable request of a data subject;

(C) specify penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unfair personal information practice;

(D) take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system;

(E) make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance

63-619 O - 76 - 39

that those requirements and limitations will be observed; except in instances when an individual specifically requests that data about him be transferred to another system or organization;

(F) maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given;

(G) maintain data in the system with which such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits, that may be made on the basis of such data.

(b) Any organization maintaining an administrative automated personal data system that publicly disseminates statistical reports or research findings based on personal data drawn from the system, or from systems of other organizations, shall—

(1) make such data publicly available for independent analysis, on reasonable terms; and

(2) take reasonable precautions to assure that no data made available for independent analysis will be used in a way that might reasonably be expected to prejudice judgments about any individual data sub-

ject's character, qualifications, rights, opportunities, or benefits.

(c) PUBLIC NOTICE REQUIREMENT.—Any organization maintaining an administrative automated personal data system shall give public notice of the existence and character of its system once each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations, in a media likely to bring attention to the evidence of the records to the data subject. Any organization maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify:

(1) The name of the system.

(2) The nature and purpose or purposes of the system.

(3) The categories and number of persons on whom data is being or is to be maintained.

(4) The categories of data being or to be maintained, indicating which categories are being or are to be stored in computer-accessible files.

(5) The organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof.

(6) The categories of data sources.

(7) A description of all types of use being or to be made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them.

(8) The procedures whereby an individual can (A) be informed if he is the subject of data in the systems; (B) gain access to such data; and (C) contest their accuracy, completeness, timeliness, pertinence, and the necessity for retaining it.

(9) The procedures whereby an individual, group, or organization can gain access to data used for statistical reporting or research in order to subject such data to independent analysis.

(10) The title, name, and address of the person immediately responsible for the system.

(11) A description of the penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings attention to any evidence of unfair information practices.

(d) RIGHTS OF INDIVIDUAL DATA SUBJECTS.—Any

organization maintaining an administrative automated personal data system shall—

(1) inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the organization, of providing or not providing such data;

(2) upon request and proper identification of any data subject, clearly and accurately disclose to the data subject, in a form comprehensible to him—

(A) all data about the data subject;

(B) the sources of the information;

(C) the recipients of any transfer, report, dissemination, or use of data about the data subject, including the identity of all persons and organizations involved and their relationship to the system;

except that the disclosure required by this paragraph shall not be applicable to subject files that are (i) directly related to international relations or international subversive activities, or to classified national defense information whose disclosure or unauthorized receipt or use constitutes a violation under any Federal criminal law, or (ii) active criminal investigatory data, except active criminal investigatory data which has been main-

tained for a period longer than reasonably necessary to bring indictment, information, or to commence prosecution.

(3) comply with the following minimum conditions of disclosure to data subjects—

(A) an organization shall make the disclosures required by paragraph (2) of this subsection during normal business hours;

(B) the disclosures required under paragraph (2) of this subsection shall be made to the data subject (i) in person if he appears in person and furnishes proper identification; in which case the data subject is entitled to personal, visual inspection of data about him; (ii) by telephone if he has made a written request, with proper identification; in which case telephone disclosures are to be made without charge to the data subject; (iii) by mail if he has made a written request, with proper identification; and (iv) by providing a copy of his file, if requested pursuant to (i), (ii), or (iii) of this clause, at a charge not to exceed 10 cents per page;

(C) the data subject shall be permitted to be accompanied by one person of his choosing, who shall furnish reasonable identification. An organization may require the data subject to furnish a writ-

ten statement granting permission to the organization to discuss the data subject's file in such person's presence.

(4) assure that no use of individually identifiable data is made that is not within the purposes of the system published under subsection (e) of this section, unless, in the case of each use of such data, the informed consent of the individual has been obtained in writing;

(5) assure, to the greatest practicable extent, that no data about an individual is made available from the system in response to a demand for data made by means of compulsory legal process, unless the individual to whom the data pertain has been notified of the demand; and

(6) if the completeness, accuracy, pertinence, timeliness, or necessity for retaining the data in the system is disputed by the data subject and the dispute is directly conveyed to the organization by the data subject, comply with the following minimum procedures:

(A) The organization shall within a reasonable period of time investigate and record the current status of that data unless it has reasonable grounds to believe that the dispute by the data subject is frivolous or irrelevant.

(B) If, after such investigation, such data is

found to be inaccurate or can no longer be verified, the organization shall promptly delete such data.

(C) The presence of contradictory information in the data subject's file does not in and of itself constitute reasonable grounds for believing the dispute is frivolous or irrelevant.

(D) If the investigation does not resolve the dispute, the data subject may file a brief statement setting forth the nature of the dispute; except that the organization may limit such statements to not more than one hundred words if the organization provides the data subject with assistance in writing a clear summary of the dispute.

(E) Whenever a statement of a dispute is filed, unless there are reasonable grounds to believe that it is frivolous or irrelevant, the organization shall, in any subsequent transfer, report, or dissemination of the data in question, clearly note that it is disputed by the data subject and provide either the data subject's statement or a clear and accurate summary thereof.

(F) Following any deletion of data which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed data, the organization shall, (i) at the request of the

data subject, furnish notification that the item has been deleted, or a statement, or summary, which contains the deleted or disputed information to any person specifically designated by the data subject; and (ii) the organization shall clearly and conspicuously disclose to the data subject his rights to make such a request.

SAFEGUARD REQUIREMENTS FOR STATISTICAL-REPORTING AND RESEARCH SYSTEM

SEC. 5. (a) GENERAL REQUIREMETS.—(1) Any organization maintaining a record of personal data, which it does not maintain as part of an automated personal data system used exclusively for statistical-reporting or research, shall make no transfer of any such data to another organization without prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an automated personal data system that is not subject to these safeguard requirements or the safeguard requirements for administrative personal data systems.

(2) Any organization maintaining an automated personal data system used exclusively for statistical-reporting or research shall—

(A) identify one person immediately responsible for the system, and make any other organizational ar-

rangements that are necessary to assure continuing attention to the fulfillment of the safeguard requirements;

(B) take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all the safeguard requirements and all the rules and procedures of the organization designed to assure compliance with them;

(C) specify penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any indivdual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unfair personal information practice;

(D) take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system;

(E) make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance that those requirements and limitations will be observed, except in instances when each of the individu-

als about whom data is to be transferred has given his prior informed consent to the transfer; and

(F) have the capacity to make fully documented data readily available for independent analysis.

(b) PUBLIC NOTICE REQUIREMENT.—Any organization maintaining an automated personal data system used exclusively for statistical-reporting or research shall give public notice of the existence and character of its system once each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations, in a media likely to bring attention to the existence of the records to the data subject. Any organization maintaining more than one such system shall publish annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify—

(1) the name of the system;

(2) the nature and purpose or purposes of the system;

(3) the categories and number of persons on whom data is being or is to be maintained;

(4) the categories of data being or to be maintained, indicating which categories are being or are to be stored in computer-accessible files;

(5) the organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof;

(6) the categories of data sources;

(7) a description of all types of use being or to be made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them;

(8) the procedures whereby an individual, group, or organization can gain access to data for independent analysis;

(9) the title, name, and address of the person immediately responsible for the system;

(10) a statement of the system's provisions for data confidentiality and the legal basis for them.

(c) RIGHTS OF INDIVIDUAL DATA SUBJECTS.—Any organization maintaining an automated personal data system used exclusively for statistical reporting or research shall—

(1) inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the

organization, of providing or not providing such data;

(2) assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless, in the case of each use of such data, the informed consent of the individual has been explicitly obtained;

(3) assure, to the greatest extent practicable, that no data about an individual is made available from the system in response to a demand for data made by means of compulsory legal process, unless the individual to whom the data pertain—

(A) has been notified of the demand, and

(B) has been afforded full access to the data before they are made available in response to the demand.

UNAUTHORIZED DISCLOSURE OF IDENTIFYING NUMBERS

SEC. 6. (a) DISCLOSURE OF SOCIAL SECURITY ACCOUNT NUMBER.—It shall be unlawful for any person to require an individual to disclose or furnish his social security account number, or other identifying number, issued under the Social Security Act, for any purpose, in connection with any business transaction or commercial or other related activity, or to refuse to extend credit or make a loan to or enter into any other business transaction or commercial relationship with an individual (except to the extent specifically neces-

sary for the conduct or administration of the old-age, survivors, and disability insurance programs) wholly or partly because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by a provision of Federal law.

(b) TECHNICAL AMENDMENTS.—(1) Section 1106(a) of the Social Security Act (42 U.S.C. 1306) is amended by inserting, immediately preceding the period in the first sentence thereof, a semicolon and "except that in no event shall disclosure of the social security account number or other identifying number of any individual to whom (or to whose wages and self-employment income any such file, record, report, paper, or information relates, be authorized pursuant to this section except with the express written permission of such individual (or as provided in subsection (c))".

(2) Such section 1106 is further amended by adding at the end thereof the following new subsection:

"(d) Social security account numbers (or other identifying numbers) issued to individuals under title II shall be issued solely for purposes of the old-age, survivors, and disability insurance program established by such title, and (except to the extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program) no individual shall be required to include the number issued to him on any form or return prescribed

for purposes of any Federal, State, or local law or to be required to disclose or furnish such number to any public officer or employee, or any other person, in connection with the conduct or administration of any program or activity under any Federal, State, or local law, unless the inclusion, disclosure, or furnishing of such number is specifically required by a provision of Federal law.

ENFORCEMENT

SEC. 7. (a) INJUNCTIONS FOR COMPLIANCE.—Whenever it appears to the Attorney General of the United States that any organization has engaged, is engaged, or is about to engage in any act or practice constituting an unfair personal information practice under this Act, he may by his own discretion bring an action, in any appropriate United States district court, to enjoin such acts or practices. If the court finds there is being or is about to be committed any such act or practice, a permanent or temporary injunction or restraining order may be granted without bond. Upon application of the Attorney General any such court may also issue an injunction requiring any organization to comply with any section of this Act.

(b) ENFORCEMENT BY PRIVATE PERSONS.—(1) Any individual aggrieved may commence a civil action in any appropriate United States district court to enforce the rights granted or protected by this Act. The court may grant as

relief, as it deems appropriate, any permanent, or temporary injunction, temporary restraining order, or other order.

(c) CIVIL LIABILITY.—In any civil action commenced under subsection (b), any individual or organization which commits an unfair personal information practice or a violation of section 6 shall be liable in an amount equal to the sum of—

(1) any actual damages sustained by the individual aggrieved as a result of the unfair practice or violation, but not less than liquidated damages of $100; and

(2) not more than $1,000 punitive damages.

(d) JURISDICTION OF COURTS; LIMITATIONS OF ACTIONS.—An action to enforce any right granted or protected under this Act may be brought in any appropriate United States district court without regard to the amount in controversy, within one hundred and eighty days from the date on which the liability arises, except that where a defendant has materially and willfully failed to comply with the safeguards under this Act, the action may be brought at any time within one hundred and eighty days after discovery by the individual data subject. Such an action may be brought in any judicial district in which the unfair practice or violation is alleged to have been committed or in which

the records relevant to such practice or violation are maintained and administered.

CRIMINAL LIABILITY OF FEDERAL OFFICERS OR EMPLOYEES

SEC. 8. Any officer or employee of any Federal agency, the courts of the United States, the governments of the territories or possessions of the United States, or the government of the District of Columbia who willfully or knowingly permits or causes to occur an unfair personal information practice shall for each offense, be fined not less than $100 nor more than $1,000 or imprisoned not more than one year, or both.

SEVERABILITY

SEC. 9. If any provision of this Act or the application thereof to any particular circumstance or situation is held invalid, the remainder of this Act or the application of such provision to any other circumstance or situation shall not be affected thereby.

EFFECTIVE DATE

SEC. 10. This Act shall take effect one year after the date of its enactment.

STATE LAWS

SEC. 11. (a) No State law in effect on the date of passage of this Act or which may become effective thereafter shall be superseded by any provision of this Act; except insofar as such State law is in conflict with this Act.

93D CONGRESS
2D SESSION

S. 2963

IN THE SENATE OF THE UNITED STATES

FEBRUARY 5, 1974

Mr. ERVIN (for himself, Mr. HRUSKA, Mr. MATHIAS, Mr. KENNEDY, Mr. BAYH, Mr. TUNNEY, Mr. YOUNG, Mr. BROOKE, Mr. MANSFIELD, Mr. ROBERT C. BYRD, Mr. BURDICK, Mr. ROTH, Mr. HUGH SCOTT, Mr. THURMOND, and Mr. FONG) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To protect the constitutional rights and privacy of individuals upon whom criminal justice information and criminal justice intelligence information have been collected and to control the collection and dissemination of criminal justice information and criminal justice intelligence information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Criminal Justice Information Control and Protection of Privacy Act of 1974".

TITLE I—FINDINGS AND DECLARATION OF POLICY; DEFINITIONS

CONGRESSIONAL FINDINGS AND DECLARATION POLICY

SEC. 101. The Congress finds and declares that the several States and the United States have established criminal justice information systems which have the capability of transmitting and exchanging criminal justice information between or among each of the several States and the United States; that the exchange of this information by Federal agencies is not clearly authorized by existing law; that the exchange of this information has great potential for increasing the capability of criminal justice agencies to prevent and control crime; that the exchange of inaccurate or incomplete records of such information can do irreparable injury to the American citizens who are the subjects of the records; that the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from misuse of these systems; that citizens' opportunities to secure employment and credit and their right to due process, privacy, and other legal protections are endangered by misuse of these systems; that in order to secure the constitutional rights guaranteed by the first amendment, fourth amendment, fifth amendment, sixth amendment, ninth amendment, and fourteenth amendment, uniform Federal legislation is necessary to govern these

systems; that these systems are federally funded, that they contain information obtained from Federal sources or by means of Federal funds, or are otherwise supported by the Federal Government; that they utilize interstate facilities of communication and otherwise affect commerce between the States; that the great diversity of statutes, rules, and regulations among the State and Federal systems require uniform Federal legislation; and that in order to insure the security of criminal justice information systems, and to protect the privacy of individuals named in such systems, it is necessary and proper for the Congress to regulate the exchange of such information.

DEFINITIONS

SEC. 102. For the purposes of this Act—

(1) "Information system" means a system, whether automated or manual, operated or leased by Federal, regional, State, or local government or governments, including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation, or dissemination of information.

(2) "Criminal justice information system" means an information system for the collection, processing, preservation, or dissemination of criminal justice information.

(3) "Criminal justice intelligence information system" means an information system for the collection, processing,

preservation, or dissemination of criminal justice intelligence information.

(4) "Automated system" means an information system that utilizes electronic computers, central information storage facilities, telecommunications lines, or other automatic data processing equipment used wholly or in part for data collection, analysis, or display as distinguished from a system in which such activities are performed manually.

(5) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, deceased, deferred disposition, dismissed-civil action, extradited, found insane, found mentally incompetent,

pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, or executive clemency.

(6) "Dissemination" means the transmission of information, whether orally or in writing.

(7) "Criminal justice information" means information on individuals collected or disseminated, as a result of arrest, detention, or the initiation of criminal proceeding, by criminal justice agencies, including arrest record information, correctional and release information, criminal history record information, conviction record information, identification record information, and wanted persons record information. The term shall not include statistical or analytical records or reports, in which individuals are not identified and from which their identities are not ascertainable. The term shall not include criminal justice intelligence information.

(8) "Arrest record information" means information concerning the arrest, detention, or commencement of criminal proceedings on an individual which does not include the disposition of the charge arising out of that arrest, detention, or proceeding.

(9) "Correctional and release information" means information on an individual compiled by a criminal justice or noncriminal justice agency in connection with bail, pretrial or posttrial release proceedings, reports on the mental condi-

tion of an alleged offender, reports on presentence investigations, reports on inmates in correctional institutions or participants in rehabilitation programs, and probation and parole reports.

(10) "Criminal history record information" means information disclosing both that an individual has been arrested or detained or that criminal proceedings have been commenced against an individual and that there has been a disposition of the criminal charge arising from that arrest, detention, or commencement of proceedings. Criminal history record information shall disclose whether such disposition has been disturbed, amended, supplemented, reduced, or repealed by further proceedings, appeal, collateral attack, or otherwise.

(11) "Conviction record information" means information disclosing that a person has pleaded guilty or nolo contendere to or was convicted on any criminal offense in a court of justice, sentencing information, and whether such plea or judgment has been modified.

(12) "Identification record information" means fingerprint classifications, voice prints, photographs, and other physical descriptive data concerning an individual which does not include any indication or suggestion that the individual has at any time been suspected of or charged with criminal activity.

(13) "Wanted persons record information" means identification record information on an individual against whom there is an outstanding arrest warrant including the charge for which the warrant was issued and information relevant to the individual's danger to the community and such other information that would facilitate the regaining of the custody of the individual.

(14) "Criminal justice intelligence information" means information on an individual on matters pertaining to the administration of criminal justice, other than criminal justice information, which is indexed under an individual's name or which is retrievable by reference to identifiable individuals by name or otherwise. This term shall not include information on criminal justice agency personnel, or information on lawyers, victims, witnesses, or jurors collected in connection with a case in which they were involved.

(15) "The administration of criminal justice" means any activity by a governmental agency directly involving the apprehension, detention, pretrial release, posttrial release, prosecution, defense adjudication, or rehabilitation of accused persons or criminal offenders or the collection, storage, dissemination, or usage of criminal justice information.

(16) "Criminal justice agency" means a court sitting in criminal session or a governmental agency created by statute or any subunit thereof created by statute, which performs

as its principal function, as expressly authorized by statute, the administration of criminal justice. Any provision of this Act which relates to the activities of a criminal justice agency also relates to any information system under its management control or any such system which disseminates information to or collects information from that agency.

(17) "Purge" means to remove information from the records of a criminal justice agency or a criminal justice information system so that there is no trace of information removed and no indication that such information was removed.

(18) "Seal" means to close a record possessed by a criminal justice agency or a criminal justice information system so that the information contained in the record is available only (a) in connection with research pursuant to section 201 (d), (b) in connection with review pursuant to section 207 by the individual or his attorney, (c) in connection with an audit pursuant to section 206, or (d) on the basis of a court order pursuant to section 205.

(19) "Judge of competent jurisdiction" means (a) a judge of a United States district court or a United States court of appeals; (b) a Justice of the Supreme Court of the United States; and (c) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing access to criminal justice information.

(20) "Attorney General" means the Attorney General of the United States.

(21) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

TITLE II—COLLECTION AND DISSEMINATION OF CRIMINAL JUSTICE INFORMATION AND CRIMINAL JUSTICE INTELLIGENCE INFORMATION

DISSEMINATION, ACCESS AND USE—GENERALLY

SEC. 201. (a) Criminal justice information may be maintained or disseminated, by compulsory process or otherwise, outside the criminal justice agency which collected such information, only as provided in this Act.

(b) Criminal justice information may be collected only by or disseminated only to officers and employees of criminal justice agencies: *Provided, however,* That beginning two years after enactment of this Act such information may be collected only by or disseminated only to officers and employees of criminal justice agencies which are expressly authorized to receive such information by Federal or State statute. Criminal justice information shall be used only for the purpose of the administration of criminal justice.

(c) Except as otherwise provided by this Act, conviction record information may be made available for purposes

other than the administration of criminal justice only if expressly authorized by applicable State or Federal statute.

(d) Criminal justice information may be made available to qualified persons for research related to the administration of criminal justice under regulations issued by the Federal Information Systems Board, created pursuant to title III. Such regulations shall require preservation of the anonymity of the individuals to whom such information relates, shall require the completion of nondisclosure agreements by all participants in such programs and shall impose such additional requirements and conditions as the Federal Information Systems Board finds to be necessary to assure the protection of privacy and security interests. In formulating regulations pursuant to this section the Board shall develop procedures designed to prevent this section from being used by criminal justice agencies to arbitrarily deny access to criminal justice information to qualified persons for research purposes where they have otherwise expressed a willingness to comply with regulations issued pursuant to this section.

DISSEMINATION OF CERTAIN CRIMINAL JUSTICE INFORMATION TO CRIMINAL JUSTICE AGENCIES

SEC. 202. (a) Except as otherwise provided in this section and in section 203, a criminal justice agency may disseminate to another criminal justice agency only conviction record information.

(b) A criminal justice agency may disseminate arrest record information on an individual to another criminal justice agency—

(1) if that individual has applied for employment at the latter agency and such information is to be used for the sole purpose of screening that application,

(2) if the matter about which the arrest record information pertains has been referred to the latter agency for the purpose of commencing or adjudicating criminal proceedings and that agency may use the information only for a purpose related to that proceeding, or

(3) if the latter agency has arrested, detained, or commenced criminal proceedings against that individual for a subsequent offense, and the arrest record information in the possession of the former agency indicates (A) that there was a prior arrest, detention, or criminal proceeding commenced occurring less than one year prior to the date of the request, and (B) that active prosecution is still pending on the prior charge. In computing the one-year period, time during which the individual was a fugitive shall not be counted. The indication of all relevant facts concerning the status of the prosecution on the prior arrest, detention, or proceeding must be sent to the latter agency and that agency may

use the information only for a purpose related to the subsequent arrest, detention, or proceeding.

(c) A criminal justice agency may disseminate criminal history record information on an individual to another criminal justice agency—

(1) if that individual has applied for employment at the latter agency and such information is to be used for the sole purpose of screening that application,

(2) if the matter about which the criminal history information pertains has been referred to the latter agency for the purpose of commencing or adjudicating criminal proceedings or for the purpose of preparing a pretrial release, posttrial release, or presentence report and that agency may use the information only for a purpose related to that proceeding or report, or

(3) if the requesting agency has arrested, detained, or commenced criminal proceedings against that individual for a subsequent offense or if the agency is preparing a pretrial release, posttrial release, or presentence report on a subsequent offense and such information is to be used only for a purpose related to that arrest, detention, or proceeding.

(d) A criminal justice agency may disseminate correctional and release information to another criminal justice agency or to the individual to whom the information per-

tains, or his attorney, where authorized by Federal or State statute.

(e) This section shall not bar any criminal justice agency which lawfully possesses arrest record information from obtaining or disseminating dispositions in order to convert that arrest record information to criminal history information. Nor shall this section bar any criminal justice information system to act as a central repository of such information so long as a State statute expressly so authorizes and so long as that statute would in no way permit that system to violate or to facilitate violation of any provision of this Act. Nor shall this section bar any criminal justice agency from supplying criminal history information to any criminal justice information system established in the Federal Government pursuant to section 307 of this Act.

DISSEMINATION OF IDENTIFICATION RECORD INFORMATION AND WANTED PERSONS RECORD INFORMATION

SEC. 203. Identification record information may be disseminated to criminal justice and to noncriminal justice agencies for any purpose related to the administration of criminal justice. Wanted persons information may be disseminated to criminal justice and noncriminal justice agencies only for the purpose of apprehending the subject of the information.

SECONDARY USE OF CRIMINAL JUSTICE INFORMATION

SEC. 204. Agencies and individuals having access to criminal justice information shall not, directly or through any intermediary, disseminate, orally or in writing, such information to any individual or agency not authorized to have such information nor use such information for a purpose not authorized by this Act: *Provided, however,* That rehabilitation officials of criminal justice agencies with the consent of the person under their supervision to whom it refers may orally represent the substance of such individuals criminal history record information to prospective employers if such representation is in the judgment of such officials and the individual's attorney, if represented by counsel, helpful to obtaining employment for such individual. In no event shall such correctional officials disseminate records or copies of records of criminal history record information to any unauthorized individual or agency. A court may disclose criminal justice information on an individual in a published opinion or in a public criminal proceeding.

METHOD OF ACCESS AND ACCESS WARRANTS

SEC. 205. (a) Except as provided in subsection 201 (d) or in subsection (b) of this section, an automated criminal justice information system may disseminate arrest record information, criminal history record information, or conviction record information on an individual only if the inquiry is

based upon positive identification of the individual by means of identification record information. The Federal Information Systems Board shall issue regulations to prevent dissemination of such information, except in the above situations, where inquiries are based upon categories of offense or data elements other than identification record information. For the purpose of this section "positive identification" means identification by means of fingerprints or other reliable identification record information.

(b) Notwithstanding the provisions of subsection (a), access to arrest record information, criminal history record information, or conviction record information contained in automated criminal justice information systems on the basis of data elements other than identification record information shall be permissible if the criminal justice agency seeking such access has first obtained a class access warrant from a State judge of competent jurisdiction, if the information sought is in the possession of a State or local agency or information system, or from a Federal judge of competent jurisdiction, if the information sought is in the possession of a Federal agency or information system. Such warrants may be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (1) such access is imperative for purposes of the criminal justice agency's responsibilities in the administration of criminal justice and

(2) the information sought to be obtained is not reasonably available from any other source or through any other method. A summary of each request for such a warrant, together with a statement of its disposition, shall within ninety days of disposition be furnished the Federal Information Systems Board by the judge.

(c) Access to criminal justice information which has been sealed pursuant to section 206 shall be permissible if the criminal justice agency seeking such access has obtained an access warrant from a State judge of competent jurisdiction if the information sought is in the possession of a State or local agency or information system, or from a Federal judge of competent jurisdiction, if the information sought is in the possession of a Federal agency or information system. Such warrants may be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (1) such access is imperative for purposes of the criminal justice agency's responsibilities in the administration of criminal justice, and (2) the information sought to be obtained is not reasonably available from any other source or through any other method.

SECURITY, ACCURACY, UPDATING, AND PURGING

SEC. 206. Each criminal justice information system shall adopt procedures reasonably designed—

(a) To insure the physical security of the system, to

63-619 O - 76 - 4

prevent the unauthorized disclosure of the information contained in the system, and to insure that the criminal justice information in the system is currently and accurately revised to include subsequently received information. The procedures shall also insure that all agencies to which such records are disseminated or from which they are collected are currently and accurately informed of any correction, deletion, or revision of the records. Such regulations shall require that automated systems shall as soon as technically feasible inform any other information system or agency which has direct access to criminal justice information contained in the automated system of any disposition relating to arrest record information on an individual or any other change in criminal justice information in the automated system's possession.

(b) To insure that criminal justice information is purged or sealed when required by State or Federal statute, State or Federal regulations, or court order, or when, based on considerations of age, nature of the record, or the interval following the last entry of information indicating that the individual is under the jurisdiction of a criminal justice agency, the information is unlikely to provide a reliable guide to the behavior of the individual. Such procedures shall, as a minimum, provide—

(1) for the prompt sealing or purging of criminal justice information relating to an individual who has been

free from the jurisdiction or supervision of any law enforcement agency for (A) a period of seven years if such individual has previously been convicted of an offense classified as a felony under the laws of the jurisdiction where such conviction occurred, or (B) a period of five years, if such individual has previously been convicted of a nonfelonious offense as classified under the laws of the jurisdiction where such conviction occurred, or (C) a period of five years if no conviction of the individual occurred during that period, no prosecution is pending at the end of the period, and the individual is not a fugitive; and

(2) for the prompt sealing or purging of criminal history record information in any case in which the police have elected not to refer the case to the prosecutor or in which the prosecutor has elected not to commence criminal proceedings.

(c) To insure that criminal justice agency personnel may use or disseminate criminal justice information only after determining it to be the most accurate and complete information available to the criminal justice agency. Such regulations shall require that, if technically feasible, prior to the dissemination of arrest record information by automated criminal justice information systems, an inquiry is automatically made of and a response received from the agency which

contributed that information to the system to determine whether a disposition is available.

(d) To insure that information may not be submitted, modified, updated, disseminated, or removed from any criminal justice information system without verification of the identity of the individual to whom the information refers and an indication of the person or agency submitting, modifying, updating, or removing the information.

ACCESS BY INDIVIDUALS FOR PURPOSES OF CHALLENGE

SEC. 207. (a) Any individual who believes that a criminal justice information system or criminal justice agency maintains criminal justice information concerning him, shall upon satisfactory verification of his identity, be entitled to review such information in person or through counsel and to obtain a certified copy of it for the purpose of challenge, correction, or the addition of explanatory material, and in accordance with rules adopted pursuant to this section, to challenge, purge, seal, delete, correct, and append explanatory material.

(b) Each criminal justice agency and criminal justice information system shall adopt and publish regulations to implement this section which shall, as a minimum, provide—

(1) the time, place, fees to the extent authorized by statute, and procedure to be followed by an individ-

ual or his attorney in gaining access to criminal justice information;

(2) that any individual whose record is not purged, sealed, modified, or supplemented after he has so requested in writing shall be entitled to a hearing within thirty days of such request before an official of the agency or information system authorized to purge, seal, modify, or supplement the criminal justice information at which time the individual may appear with counsel, present evidence, and examine and cross-examine witnesses;

(3) any record found after such a hearing to be inaccurate, incomplete, or improperly maintained shall, within thirty days of the date of such finding, be appropriately modified, supplemented, purged, or sealed;

(4) each criminal justice information system shall keep and, upon request, disclose to such person the name of all persons, organizations, criminal justice agencies, noncriminal justice agencies, or criminal justice information systems to which the date upon which such criminal justice information was disseminated;

(5) (A) beginning on the date that a challenge has been made to criminal justice information pursuant

to this section, and until such time as that challenge is finally resolved, any criminal justice agency or information system which possesses the information shall disseminate the fact of such challenge each time it disseminates the challenged criminal justice information. In the case of a challenge to criminal justice information maintained by an automated criminal justice information system, such system shall automatically inform any other information system or criminal justice agency to which such automated system has disseminated the challenged information in the past, of the fact of the challenge and its status;

(B) if any corrective action is taken as a result of a review or challenge filed pursuant to this section, any agency or system which maintains or has ever received the uncorrected criminal justice information shall be notified as soon as practicable of such correction and immediately correct its records of such information. In the case of the correction of criminal justice information maintained by an automated criminal justice information system, any agency or system which maintains or has ever received the uncorrected criminal justice information shall if technically feasible be notified immediately

of such correction and shall immediately correct its records of such information; and

(6) the action or inaction of a criminal justice information system or criminal justice agency on a request to review and challenge criminal justice information in its possession as provided by this section shall be reviewable by the appropriate United States district court pursuant to a civil action under section 308.

(c) No individual who, in accord with this section, obtains criminal justice information regarding himself may be required or requested to show or transfer records of that information to any other person or any other public or private agency or organization: *Provided, however,* That if a Federal or State statute expressly so authorizes, conviction record information may be disseminated to noncriminal justice agencies and an individual might be requested or required to show or transfer copies of records of such conviction record information to such noncriminal justice agencies.

INTELLIGENCE SYSTEMS

SEC. 208. (a) Criminal justice intelligence information shall not be maintained in criminal justice information systems.

(b) Criminal justice intelligence information shall not be maintained in automated systems.

TITLE III—ADMINISTRATIVE PROVISIONS; REGULATIONS; CIVIL REMEDIES; CRIMINAL PENALTIES

FEDERAL INFORMATION SYSTEMS BOARD

SEC. 301. (a) CREATION AND MEMBERSHIP.—There is hereby created a Federal Information Systems Board (hereinafter the "Board") which shall have overall responsibility for the administration and enforcement of this Act. The Board shall be composed of nine members. One of the members shall be the Attorney General and two of the members shall be designated by the President as representatives of other agencies outside of the Department of Justice. The six remaining members shall be appointed by the President with the advice and consent of the Senate. Of the six members appointed by the President, three shall be either directors of statewide criminal justice information systems or members of the Federal Information Systems Advisory Committee at the time of their appointment. The three remaining Presidential appointees shall be private citizens well versed in the law of privacy, constitutional law, and information systems technology. The President shall designate one of the six Presidential appointees as Chairman and such designation shall also be confirmed by the advice and consent of the Senate.

(b) COMPENSATION OF MEMBERS AND QUORUM.—Members of the Board appointed by the President shall be compensated at the rate of $100 per day for each day spent in the work of the Board, and shall be paid actual travel expenses and per diem in lieu of subsistence expenses when away from their usual places of residence, as authorized by section 5703 of title 5, United States Code. Five members shall constitute a quorum for the transaction of business.

(c) AUTHORITY.—For the purpose of carrying out its responsibilities under the Act the Board shall have authority to—

(1) issue regulations as required by section 303;

(2) review and disapprove of regulations issued by a State agency pursuant to section 304, or by any criminal justice agency which the Board finds to be inconsistent with this Act;

(3) exercise the powers set out in subsection 307 (d);

(4) bring actions under section 308 for declaratory and injunctive relief;

(5) operate an information system for the exchange of criminal justice information among the States and with the Federal Government pursuant to section 307;

(6) supervise the installation and operation of any criminal justice information system or criminal justice

intelligence information system operated by the Federal Government;

(7) conduct an ongoing study of the policies of various agencies of the Federal Government in the operation of information systems;

(8) require any department or agency of the Federal Government or any criminal justice agency to submit to the Board such information and reports with respect to its policy and operation of information systems or with respect to its collection and dissemination of criminal justice information or criminal justice intelligence information and such department or agency shall submit to the Board such information and reports as the Board may reasonably require; and

(9) conduct audits as required by section 306.

(d) OFFICERS AND EMPLOYEES.—The Board may appoint and fix the compensation of a staff director, legal counsel, and such other staff personnel as it deems appropriate.

(e) REPORT TO CONGRESS AND TO THE PRESIDENT.—The Board shall issue an annual report to the Congress and to the President. Such report shall at a minimum contain—

(1) the results of audits conducted pursuant to section 306;

(2) a summary of public notices filed by criminal

justice information systems, criminal justice intelligence information systems, and criminal justice agencies pursuant to section 305; and

(3) any recommendations the Board might have for new legislation on the operation or control of information systems or on the collection and control of criminal justice information or criminal justice intelligence information.

FEDERAL INFORMATION SYSTEMS ADVISORY COMMITTEE

SEC. 302. (a) CREATION AND MEMBERSHIP.— There is hereby created a Federal Information Systems Advisory Committee (hereinafter called the Committee) which shall advise the Board on its activities. The Committee shall be composed of one representative from each State appointed by the Governor, who shall serve at the pleasure of the Governor. However, once the State has created an agency pursuant to subsection 304 (b), the State's representative on the Committee shall be designated by that agency and shall serve at the pleasure of that agency.

(b) CHAIRMAN AND SUBCOMMITTEE.—The Committee shall be convened by the Board and at its first meeting shall elect a chairman from its membership. The Committee may create an executive committee and such other subcommittees as it deems necessary.

(c) AUTHORITY.—The Committee shall make any rec-

mmendations it deems appropriate to the Board concerning the Board's responsibilities under this Act, including its recommendations concerning regulations to be issued by the Board pursuant to section 303, concerning the Board's operation of interstate information systems pursuant to section 307, and concerning any recommendations which the Board might make in its annual report to Congress and the President.

(d) OFFICERS AND EMPLOYEES.—The Committee shall have access to the services and facilities of the Board and if the Board deems necessary the Committee shall have its own staff.

FEDERAL REGULATIONS

SEC. 303. The Board shall, after appropriate consultation with the Committee and other representatives of State and local criminal justice agencies participating in information systems covered by this Act and other interested parties, promulgate such rules, regulations, and procedures as it may deem necessary to effectuate the provisions of this Act. The Board shall follow the provisions of the Administrative Procedures Act with respect to the issuance of such rules. All regulations issued by the Board or any criminal justice agency pursuant to this Act shall be published and easily accessible to the public.

STATE REGULATIONS AND CREATION OF STATE INFORMATION SYSTEMS BOARD

SEC. 304. Beginning two years after enactment of this Act, no criminal justice agency shall collect criminal justice information from, nor disseminate criminal justice information to, a criminal justice agency—

(a) which has not adopted all of the operating procedures required by sections 206 and 207 and necessitated by other provisions of the Act; or

(b) which is located in a State which has failed to create a State information systems board. The State information systems board shall be an administrative body which is separate and apart from existing criminal justice agencies and which will have statewide authority and responsibility for:

(1) the enforcement of the provisions of this Act and any State statute which serves the same goals;

(2) the issuance of regulations, not inconsistent with this Act, regulating the exchange of criminal justice information and criminal justice intelligence information systems and the operation of criminal justice information systems and the operation of criminal justice intelligence information systems; and

(3) the supervision of the installation of criminal justice information systems, and criminal justice intelligence information systems, the exchange of information by such systems within that State and with similar systems and criminal justice agencies in other States and in the Federal Government.

PUBLIC NOTICE REQUIREMENT

SEC. 305. (a) Any criminal justice agency maintaining an automated criminal justice information system or a criminal justice intelligence information system shall give public notice of the existence and character of its system once each year. Any agency maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any agency proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall be transmitted to the Board and shall specify—

(1) the name of the system;

(2) the nature and purposes of the system;

(3) the categories and number of persons on whom data are maintained;

(4) the categories of data maintained, indicating which categories are stored in computer-accessible files;

(5) the agency's operating rules and regulations issued pursuant to sections 206 and 207, the agency's policies and practices regarding data information storage, duration of retention of information, and disposal thereof;

(6) the categories of information sources;

(7) a description of all types of use made of information, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them; and

(8) the title, name, and address of the person immediately responsible for the system.

(b) Any criminal justice agency, criminal justice information system, or criminal justice intelligence information system operated by the Federal Government shall satisfy the public notice requirement set out in subsection (a) of this section by publishing the information required by that subsection in the Federal Register.

ANNUAL AUDIT

SEC. 306. (a) At least once annually the Board shall conduct a random audit of the practices and procedures of the Federal agencies which collect and disseminate information pursuant to this Act to insure compliance with its require-

ments and restrictions. The Board shall also conduct such an audit of at least ten statewide criminal justice information systems each year and of every statewide and multistate system at least once every five years.

(b) Each criminal justice information system shall conduct a similar audit of its own practices and procedures once annually. Each State agency created pursuant to subsection 304 (b) shall conduct an audit on each criminal justice information system and each criminal justice intelligence information system operating in that State on a random basis, at least once every five years.

(c) The results of such audits shall be made available to the Board which shall report the results of such audits once annually to the Congress by May 1 of each year beginning on May 1 following the first full calendar year after the effective date of the Act.

PARTICIPATION BY THE BOARD

SEC. 307. (a) Subject to the limitations of subsections (b) and (c) of this section, the Board may participate in interstate criminal justice information systems, including the provision of central information storage facilities and telecommunications lines for interstate transmission of information.

(b) Facilities operated by the Board may include criminal history record information on an individual relating to

a violation of the criminal laws of the United States, violations of the criminal laws of two or more States, or a violation of the laws of another nation. As to all other individuals, criminal justice information included in Board facilities shall consist only of information sufficient to establish the identity of the individuals, and the identities and locations of criminal justice agencies possessing other types of criminal justice information concerning such individuals.

(c) Notwithstanding the provisions of subsection (b), the Board may maintain criminal history record information submitted by a State which otherwise would be unable to participate fully in a criminal history record information system because of the lack of facilities or procedures but only until such time as such State is able to provide the facilities and procedures to maintain the records in the State, and in no case for more than five years. Criminal history record information maintained in Federal facilities pursuant to this subsection shall be limited to information on offenses classified as felonies under the jurisdiction where such offense occurred.

(d) If the Board finds that any criminal justice information system or criminal justice agency has violated any provision of this Act, it may (1) interrupt or terminate the exchange of information as authorized by this section, or (2) interrupt or terminate the use of Federal funds for the

63-6[illegible] O - 76 - 42

operation of such a system or agency, or (3) require the system or agency to return Federal funds distributed in the past, or it may take any combination of such actions or (4) require the system or agency to discipline any employee responsible for such violation.

CIVIL REMEDIES

SEC. 308. (a) Any person aggrieved by a violation of this Act shall have a civil action for damages or any other appropriate remedy against any person, system, or agency responsible for such violation after he has exhausted the administrative remedies provided by section 207.

(b) The Board or any State agency created pursuant to subsection 304 (b) shall have a civil action for declaratory judgments, cease and desist orders, and such other injunctive relief against any criminal justice agency, criminal justice information system, or criminal justice intelligence information system within its regulatory jurisdiction.

(c) Such person, agency, or the Board may bring a civil action under this Act in any district court of the United States for the district in which the violation occurs, or in any district court of the United States in which such person resides or conducts business, or has his principal place of business, or in the District Court of the United States for the District of Columbia.

(d) The United States district court in which an action

is brought under this Act shall have exclusive jurisdiction without regard to the amount in controversy. In any action brought pursuant to this Act, the court may in its discretion issue an order enjoining maintenance or dissemination of information in violation of this Act, or correcting records of such information or any other appropriate remedy except that in an action brought pursuant to subsection (b) the court may order only declaratory or injunctive relief. In any action brought pursuant to this Act the court may also order the Board to conduct an audit of the practices and procedures of the agency in question to determine whether information is being collected and disseminated in a manner inconsistent with the provisions of this Act.

(e) In an action brought pursuant to subsection (a), any person aggrieved by a violation of this Act shall be entitled to a $100 recovery for each violation plus actual and general damages and reasonable attorneys' fees and other litigation costs reasonably incurred. Exemplary and punitive damages may be granted by the court in appropriate cases brought pursuant to subsection (a). Any person, system, or agency responsible for violations of this Act shall be jointly and severally liable to the person aggrieved for damages granted pursuant to this subsection. Any criminal justice information system or any criminal justice intelligence information system which facilitates the transfer of informa-

tion in violation of this Act shall be jointly and severally liable along with any criminal justice agency or person responsible for a violation of this Act.

(g) For the purposes of this Act the United States shall be deemed to have consented to suit and any agency or system operated by the United States, found responsible for a violation shall be liable for damages, reasonable attorneys' fees, and litigation cost as provided in subsection (f) notwithstanding any provisions of the Federal Tort Claims Act.

CRIMINAL PENALTIES

SEC. 309. Whoever willfully disseminates, maintains, or uses information knowing such dissemination, maintenance, or use to be in violation of this Act shall be fined not more than $5,000 or imprisoned for not more than five years, or both.

PRECEDENCE OF STATE LAWS

SEC. 310. (a) Any State law or regulation which places greater restrictions upon the dissemination of criminal justice information or criminal justice intelligence information or the operation of criminal justice information systems or criminal justice intelligence information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in this Act shall

take precedence over this Act or regulations issued pursuant to this Act.

(b) Any State law or regulation which places greater restrictions upon the dissemination of criminal justice information or criminal justice intelligence information or the operation of criminal justice information systems or criminal justice intelligence information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in the State law or regulations of another State shall take precedence over the law or regulations of the latter State where such information is disseminated from an agency or information system in the former State to an agency, information system, or individual in the latter State. Subject to court review pursuant to section 308, the Board shall be the final authority to determine whether a State statute or regulation shall take precedence under this section and shall as a general matter have final authority to determine whether any regulations issued by a State agency, a criminal justice agency, or information system violate this Act and are therefore null and void.

APPROPRIATIONS AUTHORIZED

SEC. 311. For the purpose of carrying out the provisions of this Act there are authorized to be appropriated such sums as the Congress deems necessary.

SEVERABILITY

SEC. 312. If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

REPEALERS

SEC. 313. The second paragraph under the headings entitled "Federal Bureau of Investigation; Salaries and Expenses" contained in the "Department of Justice Appropriations Act, 1973" is hereby repealed.

EFFECTIVE DATE

SEC. 314. The provisions of this Act shall take effect upon the date of expiration of the one-hundred-and-eighty-day period following the date of the enactment of this Act: *Provided, however,* That section 311 of this Act shall take effect upon the date of enactment of this Act.

93D CONGRESS
2D SESSION

S. 3116

IN THE SENATE OF THE UNITED STATES

MARCH 6, 1974

Mr. HATFIELD introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To protect the individual's right to privacy by prohibiting the sale or distribution of certain information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That (a) title 18, United States Code, is amended by inserting after chapter 87 a new chapter as follows:

"Chapter 88.—PRIVACY

"Sec.
"1801. Sale or distribution of personal information.

"§ 1801. Sale or distribution of personal information

"(a) Whoever, by any facility of interstate or foreign commerce or the mails, knowingly sells or distributes, or offers or attempts to sell or distribute—

"(1) a list of names or addresses, or names and addresses, of individuals;

"(2) information concerning the personal or financial condition or activities of an individual; or

"(3) information concerning the personal or real property of an individual;

without the consent of any individual to whom such list or information relates, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

"(b) This section shall not apply to—

"(1) any such sale, distribution, or such offer or attempt, if a Federal statute specifically authorizes the sale or distribution of that type of list or information;

"(2) any such sale, distribution, or such offer or attempt, to any department or agency of the United States Government or of any State or local government if that list or information is to be used only for law enforcement or national security purposes;

"(3) any such sale, distribution, or such offer or attempt, if the list or information constitutes only an insubstantial portion of a document, publication, newspaper, writing, or other means of communication;

"(4) any such distribution of, or offer or attempt to distribute, a telephone directory which contains only names, addresses, and telephone numbers, and which is

published (A) by a regulated telephone utility company (if that company does not list in such directory the name, address, or telephone number of any individual who has requested that such information not be listed), (B) by a person engaged in interstate or foreign commerce (if that person does not list in such directory the name, address, or telephone number of any individual who is not an officer or employee of that person), or (C) by a department or agency of the United States Government or of a State or local government (if that department or agency does not list in such directory the name, address, or telephone number of any individual who is not an officer or employee of a department or agency of any such government)."

(b) The table of chapters of part I of such title is amended by inserting after item 87 the following new item:

"88. Privacy ---------- 1801".

93D CONGRESS
2D SESSION

S. 3633

IN THE SENATE OF THE UNITED STATES

JUNE 12, 1974

Mr. ERVIN (for himself, Mr. BAYH, Mr. GOLDWATER, Mr. KENNEDY, and Mr. MATHIAS) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To protect the constitutional right of privacy of individuals concerning whom identifiable information is recorded by enacting principles of information practices in furtherance of articles I, III, IV, V, IX, X, and XIV of amendment to the United States Constitution.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

SECTION 1. This Act may be cited as the "Government Data Bank Right to Privacy Act".

FINDINGS AND DECLARATION OF POLICY

SEC. 2. (a) The Congress finds—

(1) that an individual's privacy is directly affected by the extensive collection, maintenance, use, and dissemination of personal information;

(2) that the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

(3) that an individual's opportunities to secure employment, insurance, credit, and his right to due process and other legal protections are endangered by these personal information systems;

(4) that in order to preserve the rights guaranteed by the first, third, fourth, fifth, ninth, and fourteenth amendments of the United States Constitution, uniform Federal legislation is necessary to establish procedures to govern information systems containing records on individuals;

(5) that these systems are federally operated or controlled, or federally funded, that they contain information obtained from Federal sources or by means of Federal funds, or are otherwise supported by the Federal Government;

(6) that they utilize interstate facilities of communication and otherwise affect commerce between the States;

(7) that the great diversity of statutes, rules, and regulations among the State and Federal systems require uniform Federal legislation;

(8) that the right of privacy is a personal and fundamental right of Federal citizenship granted and secured by the Constitution of the United States; and

(9) that in order to insure the security of information systems, and to protect the privacy of individuals named in such systems, it is necessary and proper for the Congress to regulate the exchange of such information.

(b) The purpose of this Act is to insure safeguards for personal privacy from recordkeeping organizations by adherence to the following principles of information practice:

(1) There should be no personal information system whose existence is secret.

(2) Information should not be collected unless the need for it has been clearly established in advance.

(3) Information should be appropriate and relevant to the purpose for which it has been collected.

(4) Information should not be obtained by fraudulent or unfair means.

(5) Information should not be used unless it is accurate and current.

(6) There should be a prescribed procedure for an individual to learn the information stored about him, the

purpose for which it has been recorded, and particulars about its use and dissemination.

(7) There should be a clearly prescribed procedure for an individual to correct, erase, or amend inaccurate, obsolete, or irrelevant information.

(8) Any organization holding personal information should assure its reliability and take precautions to prevent its misuse.

(9) There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent.

(10) The Federal Government should not collect personal information except as authorized by law.

DEFINITIONS

SEC. 3. As used in this Act—

(1) the term "information system" means the total components and operations of a recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars;

(2) the term "personal information" means all information that describes, locates or indexes anything about an individual including his education, financial transactions, medical history, criminal, or employment

record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

(3) the term "data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system;

(4) the term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means;

(5) the term "organization" means any Federal agency; the government of the District of Columbia; and any authority of any State, local government, or other jurisdiction;

(6) the term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization; and

(7) the term "Federal agency" means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof.

SAFEGUARD REQUIREMENTS FOR PERSONAL INFORMATION FOR ADMINISTRATIVE, STATISTICAL-REPORTING AND RESEARCH PURPOSES

SEC. 4. (a) ADMINISTRATIVE REQUIREMENTS.—Any organization maintaining an information system that includes personal information shall—

(1) collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization;

(2) collect information to the greatest extent possible from the data subject directly;

(3) establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

(4) maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

(5) make no dissemination to another system without (A) specifying requirements for security and the use of information exclusively for the purposes set forth in the notice required under subsection (c) including limitations on access thereto, and (B) determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed;

(6) transfer no personal information beyond the jurisdiction of the United States without specific authorization from the data subject or pursuant to a treaty or executive agreement in force guaranteeing that any foreign government or organization receiving personal information will comply with the applicable provisions of this Act with respect to that personal information;

(7) afford any data subject of a foreign nationality, whether residing in the United States or not, the same rights under this Act as American citizens;

(8) maintain a list of all persons having regular access to personal information in the information system;

(9) maintain for a reasonable time related to the purposes of the particular system a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority;

(10) take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this Act, the rules and procedures, including penalties for noncompliance, of the organization designed to assure compliance with such requirements;

(11) establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;

(12) comply with the written request of any individual who receives a communication in the mails, over the telephone, or in person, who believes that his name or address is available because of his inclusion on a mailing list, to remove his name and address from that list; and

(13) collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects unless expressly authorized by statute.

(b) SPECIAL ADDITIONAL REQUIREMENTS FOR STATISTICAL-REPORTING AND RESEARCH INFORMATION SYSTEMS.—(1) Any organization maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of other organizations, shall—

(A) make available to any data subject or group, without revealing trade secrets, methodology and materials necessary to validate statistical analyses, and

(B) make no materials available for independent analysis without guarantees that no personal information will be used in a way that might prejudice judgments about any data subject.

63-619 O - 76 - 43

(2) No Federal agency shall—

(A) require any individual to disclose for statistical purposes any personal information unless such disclosure is required by a constitutional provision or Act of Congress, and the individual is so informed;

(B) request any individual voluntarily to disclose personal information unless such request has been specifically authorized by Act of Congress, and the individual shall be advised that such disclosure is voluntary;

(C) make available to any non-Federal person any statistical studies or reports or other compilations of information derived by mechanical or electrical means from files containing personal information, or no manual or computer material relating thereto, except those prepared, published, and made available for general public use; and

(D) publish statistics of taxpayer income classified, in whole or in part, on the basis of a coding system for the delivery of mail.

(3) Any organization maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of other organizations, and which purges the names, personal numbers, or other identifying particulars of

individuals and certifies to the Federal Privacy Board that no inferences may be drawn about any individual, shall be exempt from the requirements of section 4(a) (3) and (4), and section 4 (c) and (d) (1) and (2).

(c) PUBLIC NOTICE REQUIREMENT.—Any organization maintaining or proposing to establish an information system for personal information shall—

(1) give notice of the existence and character of each existing system once a year to the Federal Privacy Board;

(2) give public notice of the existence and character of each existing system each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations in local or regional printed media likely to bring attention to the existence of the records to data subjects;

(3) publish such annual notices for all its existing systems simultaneously;

(4) in the case of a new system, or the substantial modification of an existing system, shall give public notice and notice to the Federal Privacy Board within a reasonable time but in no case less than three months, in advance of the initiation or modification to assure individuals who may be affected by its operation a reasonable opportunity to comment;

(5) shall assure that public notice given under this subsection specifies the following:

(A) The name of the system.

(B) The general purpose of the system.

(C) The categories of personal information, and approximate number of persons on whom information is maintained.

(D) The categories of information maintained, confidentiality requirements, and access controls.

(E) The organization's policies and practices regarding information storage, duration of retention, and purging thereof.

(F) The categories of data maintained, indicating which categories are stored in computer-accessible files, and the categories of all information sources.

(G) A description of types of use made of information including all classes of users and the organizational relationships among them.

(H) The procedures whereby an individual can—

(i) be informed if he is the subject of information in the system;

(ii) gain access to such information; and

(iii) contest the accuracy, completeness, timeliness, pertinence, and the necessity for retention.

(I) The procedures whereby an individual or group can gain access to the information system used for statistical reporting or research in order to subject them to independent analysis.

(J) The business address and telephone number of the person immediately responsible for the system; and

(6) prepare and publish a privacy impact statement describing the consequences to the individual, including his rights, privileges, benefits, detriments, and burdens, of the proposed data system, or in the case of an existing system, any proposed expansion.

(d) RIGHTS OF DATA SUBJECTS.—Any organization maintaining personal information shall—

(1) inform an individual asked to supply personal information whether he is legally required, or may refuse, to supply the information requested, and also of any specific consequences which are known to the organization, of providing or not providing such information;

(2) request permission of a data subject to disseminate part or all of this information to another organization or system not having regular access authority, and

indicate the use for which it is intended, and the specific consequences for the individual, which are known to the organization, of providing or not providing such permission;

(3) upon request and proper identification of any data subject, grant such subject the right to inspect, in a form comprehensible to such individual—

(A) all personal information about that data subject except in the case of medical information, when such information shall, upon written authorization, be given to a physician designated by the data subject;

(B) the nature of the sources of the information; and

(C) the recipients of personal information about the data subject including the identity of all persons and organizations involved and their relationship to the system when not having regular access authority.

(4) comply with the following minimum conditions of disclosure to data subject:

(A) An organization shall make disclosures to data subjects required under this Act, during normal business hours.

(B) The disclosures to data subjects required under this Act shall be made (i) in person, if he appears in person and furnishes proper identification, (ii) by mail, if he has made a written request, with proper identification, at reasonable standard charges for document search and duplication.

(C) The data subject shall be permitted to be accompanied by one person of his choosing, who must furnish reasonable identification. An organization may require the data subject to furnish a written statement granting permission to the organization to discuss that individual's file in such preson's presence.

(5) if the data subject gives notice that he wishes to challenge, correct, or explain information about him in the information system, the following minimum procedures shall be followed:

(A) The organization maintaining the information system shall investigate and record the current status of that personal information.

(B) If, after such investigation, such information is found to be incomplete, inaccurate, not pertinent, not timely nor necessary to be retained, or can no longer be verified, it shall be promptly purged.

(C) If the investigation does not resolve the dispute, the data subject may file a statement of reasonable length setting forth his position.

(D) Whenever a statement of dispute is filed, the organization maintaining the information system shall, in any subsequent dissemination or use of the information in question, clearly note that it is disputed and supply the statement of the data subject along with the information.

(E) The organization maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request.

(F) Following any correction or purging of personal information the organization shall at the request of the data subject, take reasonable steps to furnish to past recipients notification that the item has been purged or corrected.

(G) In the case of a failure to resolve a dispute, the organization shall advise the data subject of his right to request the assistance of the Federal Privacy Board.

(e) NOTIFICATION PROCEDURE.—Not later than two years from the effective date of this Act, and not less than once each year, each organization that maintains a personal information system on a data subject shall include, in any

regular communication by mail to such data subject, a written notification which includes the following:

(1) The notice shall describe the type of information held in their system or systems, expected uses allowed or contemplated.

(2) The notice shall provide the name and full address of the place where the data subject may obtain personal information pertaining to him, and in the system.

(f) Data subjects of archival-type inactive files, records, or reports shall be notified by mail of the reactivation, accessing, or reaccessing not later than six months after the date of the enactment of this Act.

(g) This Act applies to any information system which—

(1) is operated by the Federal Government; or

(2) is operated by a State or local government and funded in whole or in part by the Federal Government, or relies in whole or in part on interstate channels of communication.

EXEMPTIONS TO APPLICATIONS OF REQUIREMENTS

SEC. 5. The provisions of this Act shall not be applicable to personal information systems—

(1) to the extent that information in such systems is maintained by a Federal agency, and the President determines by Executive order that the application of

the Act, or specified parts thereof, would seriously damage national defense; and

(2) which are subject to State or Federal statutes affording substantially the same or greater protection for individual privacy; including but not limited to the right to enforce by appropriate civil action in court any violation of said statute.

USE OF SOCIAL SECURITY NUMBER

SEC. 6. It shall be unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual (except to the extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program) wholly or partly because such individual does not disclose or furnish such number unless the disclosure or furnishing of such number is specifically required by Federal law.

FEDERAL PRIVACY BOARD

SEC. 7. (a) ESTABLISHMENT.—There is an office in the General Accounting Office which shall be called the Federal Privacy Board (hereinafter in this section referred to as the "Board").

(b) MEMBERSHIP.—The Board shall consist of five members, each serving for a term of three years, three of whom shall constitute a quorum. No member shall serve more than two terms. The members of the Board shall be appointed by the Comptroller General of the United States. No more than three of the members appointed to serve at the same time shall be of the same political party. Each member shall be appointed from the public at large and not from among officers or employees of the United States. Membership on the Board shall be the sole employment of each member.

(c) COMPENSATION.—Members of the Board shall be compensated at the rate provided for GS–18 under section 5332 of title 5 of the United States Code.

(d) CHAIRMAN.—The Chairman of the Board shall be elected by the Board every two years.

(e) STAFF.—The Comptroller General shall appoint and fix the compensation of such personnel as are necessary to the carrying out of its duties.

FUNCTIONS OF THE BOARD

SEC. 8. The Board shall—

(1) publish an annual Data Base Directory of the United States containing the name and characteristics of each personal information system covered by section 4(g);

(2) make rules to assure compliance with this Act;

(3) perform or cause to be performed such research activities as may become necessary to implement this Act, and to assist organizations in complying with this Act;

(4) be granted admission at reasonable hours to premises where any information system is kept or where computers or equipment or recordings for automatic data processing are kept, and may by subpena compel the production of documents relating to such information system or such processing as is necessary to carry out its duties, but no personal information shall be compelled to be produced without the prior consent of the data subject to which it pertains. Enforcement of any subpena issued under this section shall be had in the appropriate United States district court;

(5) upon the determination of a violation of a provision of this Act or regulation promulgated under the Act, the Board may, after opportunity for a hearing, order the organization violating such provision to cease and desist such violation. The Comptroller General may enforce any order issued under this paragraph in a civil action in the appropriate United States district court;

(6) shall delegate its authority under this Act, with respect to information systems within the Federal

Government, a State, or the District of Columbia, to such State or District, which are governed by express statutory law which affords the minimum standards for the protection of privacy provided for by this Act.

(7) conduct open, public hearings on all petitions for exceptions or exemptions from provisions, application, or jurisdiction of this Act. The Board shall have no authority to make such exceptions or exemptions but shall submit appropriate reports and recommendations to Congress;

(8) issue an annual report of its activities to the Congress and the President; and

(9) recommend to Congress that a particular Federal data bank proposed to be created, expanded, or modified, because of its size, scope, sensitivity of data, or impact on privacy, should not be established except by specific legislative authorization.

TRADE SECRETS

SEC. 9. In connection with any dispute over the application of any provision of this Act, no organization shall reveal any personal information or any professional, proprietary, or business secrets; except as is required under this Act. All disclosures so required shall be regarded as confidential by those to whom they are made.

CRIMINAL PENALTY

SEC. 10. Any organization or responsible officer of an organization who willfully—

(1) keeps an information system without having notified the Federal Privacy Board; or

(2) issues personal information in violation of this Act;

shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 11. (a) INJUNCTIONS FOR COMPLIANCE.—The Attorney General of the United States, on the advice of the Federal Privacy Board, or any aggrieved person, may bring an action in the appropriate United States district court against any person who has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this Act or rules of the Federal Privacy Board, to enjoin such acts or practices.

(b) CIVIL LIABILITY FOR UNFAIR PERSONAL INFORMATION PRACTICE.—Any person, system, or agency which violates the provisions of the Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

(1) any actual damages sustained by an individual plus $100 for each violation;

(2) punitive damages where appropriate;

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

The United States consents to be sued under this section without limitation on the amount in controversy.

(c) No action shall lie under subsection (b) of this section with respect to any system subject to a statute which satisfies the provisions of section 12 or of subsection 5(b).

PRECEDENCE OF OTHER FEDERAL AND STATE LAWS

SEC. 12. Any Federal or State law, or regulation which places greater restrictions upon the dissemination of personal information or the operation of personal information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in this Act shall take precedence over this Act or regulations issued pursuant to this Act.

SEVERABILITY

SEC. 13. If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

EFFECTIVE DATE

SEC. 14. This Act shall take effect one year after the date of its enactment.

93D CONGRESS
1ST SESSION

H. R. 1281

IN THE HOUSE OF REPRESENTATIVES

JANUARY 3, 1973

Mr. CHARLES H. WILSON of California introduced the following bill; which was referred to the Committee on Post Office and Civil Service

A BILL

To amend title 5, United States Code, to protect civilian employees of the executive branch of the United States Government in the enjoyment of their constitutional rights, to prevent unwarranted governmental invasions of their privacy, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That (a) chapter 71 of title 5, United States Code, is amended by adding at the end thereof the following new subchapter III:

"SUBCHAPTER III—EMPLOYEE RIGHTS

"§ 7171. Policy

"It is the policy of the United States, as an employer, to assure that those officials of Executive agencies charged

with administrative or supervisory responsibility recognize and protect the personal and individual rights, entitlements, and benefits of employees of, and applicants for employment in, Executive agencies.

"§ 7172. Definition

"For the purpose of this subchapter, 'official of an Executive agency' means—

"(1) an officer of an Executive agency;

"(2) an 'officer' of any of the 'uniformed services' as such terms are defined under section 101 of title 37; and

"(3) an individual acting or purporting to act under the authority of an officer referred to in paragraph (1) or (2) of this section.

"§ 7173. Employee rights

"(a) An official of an Executive agency may not—

"(1) require or request, or attempt to require or request, an employee of an Executive agency or an applicant for employment in an Executive agency to disclose his race, religion, or national origin, or the race, religion, or national origin of any of his forebears. This paragraph does not prohibit inquiry concerning—

"(A) the citizenship of an employee or applicant;

"(B) the national origin of an employee or

applicant when that inquiry is considered necessary or advisable to determine suitability for assignment to activities or undertakings related to the national security of the United States or to law enforcement or to activities or undertakings of any nature outside the United States;

"(C) the race, religion, or national origin of an employee or applicant when that matter is in issue in an allegation or complaint of discrimination; or

"(D) the race, religion, or national origin of an employee or applicant when (i) that matter is directly related to or an integral part of scientific research or program evaluation, (ii) appropriate safeguards have been instituted to preserve both the voluntary participation and the anonymity of the employee or applicant, and (iii) the inquiry has been approved by the Civil Service Commission.

This paragraph does not prohibit an inquiry made to satisfy the requirements of law providing preference for Indians in connection with functions or services affecting Indians;

"(2) coerce, require, or request, or attempt to coerce, require, or request, an employee of an Executive agency to attend or participate in a formal or informal meeting, assemblage, or other group activity held to

present, advocate, develop, explain, or otherwise cover in any way, by lecture, discussion, discourse, instruction, visual presentation, or otherwise, any matter or subject other than—

"(A) the performance of official duties to which that employee is or may be assigned in the Executive agency; or

"(B) the development of skills, knowledge, or abilities that qualify him for the performance of those official duties;

"(3) coerce, require, or request, or attempt to coerce, require, or request, an employee of an Executive agency to—

"(A) participate in any way in an activity or undertaking unless it is related to the performance of official duties to which the employee is or may be assigned in the Executive agency or related to the development of skills, knowledge, or abilities that qualify him for the performance of those official duties; or

"(B) make any report concerning any activity or undertaking of the employee not involving his official duties, except—

"(i) when there is reason to believe that the activity or undertaking conflicts with, or

adversely affects the performance of, his official duties; or

"(ii) as authorized to the contrary under paragraph (6) of this subsection.

This paragraph does not prohibit the use of appropriate publicity to inform employees of requests for assistance from public service programs or organizations;

"(4) require or request, or attempt to require or request, an employee of an Executive agency or an applicant for employment in an Executive agency to submit to an interrogation or examination or to take a polygraph or psychological test designed to elicit from the employee or applicant information concerning his personal relationship with any individual related to him by blood or marriage, his religious beliefs or practices, or his attitude or conduct with respect to sexual matters. This paragraph does not prohibit—

"(A) a physician from eliciting this information or authorizing these tests in the diagnosis or treatment of an employee or applicant in individual cases and not pursuant to general practice or regulation governing the examination of employees or applicants, when the physician considers the information necessary to enable him to determine

whether or not the employee or applicant is suffering from mental illness;

"(B) an official of an Executive agency from advising an employee or applicant of a specific charge of sexual misconduct made against the employee or applicant and giving him a full opportunity to refute the charge; or

"(C) an official of an Executive agency from eliciting, from an employee or applicant, in individual cases and not pursuant to general practice or regulation, information concerning the personal relationship of the employee or applicant with any individual related to him by blood or marriage, when that official considers the information necessary in the interest of national security;

"(5) coerce or require, or attempt to coerce or require, an employee of an Executive agency to invest his earnings in bonds or other obligations or securities issued by the United States or by an Executive agency, or to make donations to any institution or cause of any kind. This paragraph does not prohibit an official of an Executive agency from calling meetings and taking any action appropriate to inform an employee of the opportunity—

"(A) voluntarily to invest his earnings in

bonds or other obligations or securities issued by the United States or by an Executive agency; or

"(B) voluntarily to make donations to any institution or cause;

"(6) require or request, or attempt to require or request, an employee of an Executive agency (other than a Presidential appointee) to disclose his property or the property of any member of his family or household. This paragraph does not prohibit—

"(A) the Department of the Treasury or any other Executive agency from requiring an employee to make such reports as may be necessary or appropriate for the determination of his liability for taxes, tariffs, customs duties, or similar obligations to the United States; or

"(B) an official of an Executive agency from requiring an employee who participates (other than in a clerical capacity) in any determination with respect to—

"(i) a Government contract or grant;

"(ii) the regulation of non-Federal enterprise;

"(iii) the tax or other liability of any person to the United States; or

"(iv) a claim that requires expenditure of money of the United States;

from disclosing specific items of the property of that employee, or specific items of the property of any member of his family or household, which may tend to indicate a conflict of interest with respect to the performance of any of the official duties to which the employee is or may be assigned.

As used in this paragraph, 'property' includes items of property, income, and other assets, and the source thereof, liabilities, and personal and domestic expenditures;

"(7) prohibit or restrict, or attempt to prohibit or restrict, the exercise by an employee of an Executive agency of the right of reasonable communication with any official of his agency; or

"(8) remove, suspend or furlough from duty without pay, demote, reduce in rank, seniority, status, pay, or performance or efficiency rating, deny promotion to, relocate, reassign, discipline, or discriminate in regard to any employment right, entitlement, or benefit or any term or condition of employment of, an employee of an Executive agency, or threaten to commit any of those acts, by reason of—

"(A) the refusal or failure of the employee

to submit to or comply with any requirement, request, or action prohibited by this subsection; or

"(B) the exercise by the employee of any right, entitlement, benefit, or other protection granted or secured by this section and section 7175 of this title.

"(b) The provisions of subsection (a) of this section do not apply to—

"(1) the Central Intelligence Agency;

"(2) the National Security Agency;

"(3) the Federal Bureau of Investigation; or

"(4) any other Executive agency, or part thereof, as the President, in the interest of national security, may recommend to the Congress.

The exemption recommended by the President and transmitted to the Congress under paragraph (4) of this subsection shall become effective at the end of the first period of 30 calendar days of continuous session of the Congress after the date on which the recommendation is transmitted unless, between the date of transmittal and the end of the 30-day period, either the committee of the House of Representatives or the committee of the Senate to which the recommendation has been referred adopts a resolution which specifically disapproves the exemption so recommended and trans-

mitted. The continuity of a session is broken only by an adjournment of the Congress sine die. The days on which either House is not in session because of an adjournment of more than 3 days to a day certain are excluded in the computation of the 30-day period.

"(c) (1) An employee of, or an applicant for employment in, an Executive agency who claims to be aggrieved by a violation or threatened violation of subsection (a) of this section is entitled to file a grievance with the agency concerned not later than 15 days after the date of the violation or threatened violation.

"(2) If—

"(A) the decision on the grievance by the Executive agency is adverse to the employee or applicant; or

"(B) after 60 days from the date the grievance is filed the Executive agency has not issued a decision on the grievance;

the employee or applicant is entitled to file a complaint with the Board on Employee Rights not later than 15 days after the adverse decision or the expiration of the 60-day period, as the case may be.

"§ 7174. Board on Employee Rights

"(a) There is hereby established a Board on Employee Rights composed of three members appointed by the President, by and with the advice and consent of the Senate, one

of whom shall be a representative of a labor organization, or association of supervisors, representing employees. Not more than two members of the Board may be adherents of the same political party and none of the members of the Board may hold another office or position in the Government of the United States. The President shall from time to time designate one of the members as chairman.

"(b) The term of office of each member of the Board is 6 years. A member appointed to fill a vacancy occurring before the end of the term of office of his predecessor serves for the remainder of that term. When the term of office of a member ends, he may continue to serve until his successor is appointed and has qualified. The President may remove a member only for inefficiency, neglect of duty, or malfeasance in office.

"(c) Two members of the Board constitute a quorum for the transaction of business.

"(d) The Board may appoint and fix the pay of such officers, attorneys, and employees, and make such expenditures, as may be necessary to carry out its functions.

"(e) The Board shall prescribe rules and regulations necessary and proper to carry out its functions under this subchapter. To the extent consistent with efficient and economical administration and the attainment and achievement of justice in the consideration and disposition of matters be-

fore the Board, the rules and regulations shall provide for the use of depositions of witnesses. The rules and regulations shall also prescribe the maximum attorney's remuneration which may be awarded under section 7176(c) of this title for services performed in connection with any matter before the Board, or the court, or both, under this subchapter. The Board may require, by subpena or otherwise, the attendance and testimony of witnesses, and the production of such books, records, correspondence, memoranda, papers, and documents, as it considers necessary.

"(f) (1) The Board shall receive and investigate written complaints, filed under section 7173(c) of this title, from or on behalf of an employee or applicant claiming to be aggrieved by a violation or threatened violation of section 7173(a) of this title. On receipt of such a complaint, the Board forthwith shall transmit a copy thereof to the head of the Executive agency concerned.

"(2) If the Board determines, within 10 days after its receipt of the complaint, that the facts alleged in the complaint do not constitute a violation or threatened violation of section 7173(a) of this title with respect to the employee or applicant, it may dismiss the complaint without a hearing. If the Board dismisses the complaint, it shall notify all interested parties of the dismissal.

"(3) If the Board does not dismiss the complaint within 10 days after its receipt thereof, it shall—

"(A) conduct a hearing on the complaint within 30 days after its receipt of the complaint; and

"(B) furnish notice of the time, place, and nature of the hearing thereon to all interested parties.

If a hearing on the complaint is to be conducted—

"(i) the Executive agency concerned shall file an answer to the complaint and participate as a party in the hearing; and

"(ii) any official of that agency, who is alleged, in the complaint or during the course of the hearing, to have committed a violation or threatened violation of section 7173(a) of this title, is entitled, in his individual capacity, to file an answer to the allegation and participate as a party in the hearing.

"(4) The Board shall render its final decision with respect to any complaint within 30 days after the conclusion of its hearing thereon.

"(g) With the written consent of the employee or applicant concerned, filed with the Board, an officer or representative of not more than one labor organization, or association of supervisors, representing employees shall be given an opportunity to participate in each hearing conducted un-

der this section, through submission of written data, views, or arguments, and, in the discretion of the Board, with opportunity for oral presentation.

"(h) Insofar as consistent with the purposes of this section, the provisions of subchapter II of chapter 5 of this title apply to the rulemaking, hearing, and adjudication functions of the Board under this section.

"(i) If, after hearing, the Board determines that a violation of section 7173(a) of this title has not occurred or is not threatened, the Board shall state its determination and notify all interested parties of the determination. Each such determination, including a dismissal by the Board of the complaint without a hearing, constitutes a final decision of the Board for purposes of judicial review.

"(j) If, after hearing, the Board determines that a violation of section 7173(a) of this title has been committed or threatened by an official of an Executive agency not subject to chapter 47 of title 10, the Board—

"(1) shall immediately issue and cause to be served on the official an order requiring him to cease and desist from the unlawful act or practice which constitutes a violation;

"(2) shall immediately endeavor to eliminate any such unlawful act or practice by informal methods of conference, conciliation, and persuasion; and

"(3) may, without regard to chapter 75 of this title—

"(A) (i) in the case of the first offense by such an official, other than any official appointed by the President, by and with the advice and consent of the Senate, issue an official reprimand against the official or order the suspension without pay of the official from the position or office held by him for a period of not to exceed 15 days; and

"(ii) in the case of a second or subsequent offense by such official, order the suspension without pay of the official from the position or office held by him for a period of not less than 15 nor more than 60 days or, when the Board considers such second or subsequent offense to be sufficiently serious to warrant such action, order the removal of the official from the position or office; and

"(B) in the case of any offense by such an official appointed by the President, by and with the advice and consent of the Senate, transmit a report concerning the violation to the President and the Congress.

A reprimand or order under subparagraph (3) (A) of this subsection shall not become effective until the expiration of the period within which the official aggrieved by the repri-

mand or order may file a petition for review or complaint for trial de novo or, if such a petition or complaint is filed, until the court makes a final disposition of the case.

"(k) If, after hearing, the Board determines that a violation of section 7173(a) of this title has been committed or threatened by an official of an Executive agency subject to chapter 47 of title 10, the Board shall—

"(1) submit a report thereon to the Secretary of the military department concerned;

"(2) endeavor to eliminate any unlawful act or practice which constitutes such a violation by informal methods of conference, conciliation, and persuasion; and

"(3) refer its determination and the record in the case to the Secretary concerned, as defined in section 101 of title 10, who shall take immediate steps to dispose of the matter under chapter 47 of title 10.

However, the immediate steps referred to in paragraph (3) of this subsection shall not be taken by the Secretary concerned until the expiration of the period within which the official aggrieved by the reference to the Secretary by the Board under that paragraph may file a petition for review or complaint for trial de novo or, if such a petition or complaint is filed, until the court makes a final disposition of the case.

"(l) (1) The Board shall submit, not later than March 31 of each year, to the President for transmittal to the Con-

gress a report on its activities under this subchapter during the immediately preceding calendar year, including—

"(A) the types and kinds of complaints filed with the Board;

"(B) the determinations, orders, and actions of the Board with respect to those complaints;

"(C) the name of each official of an Executive agency with respect to whom any action was taken or penalty imposed under subsection (j) of this section;

"(D) the nature of that action or penalty; and

"(E) such other matters as the Board considers relevant and appropriate to provide full and complete information with respect to the operation and administration of this subchapter.

"(2) The Secretary of each military department shall submit, not later than March 31 of each year, to the President for transmittal to the Congress, a report on his activities under this subchapter during the immediately preceding calendar year, including—

"(A) the disposition, under chapter 47 of title 10, of matters referred to the Secretary under paragraph (3) of subsection (k) of this section;

"(B) the name of each official of an Executive agency with respect to whom any action was taken or penalty imposed under such chapter;

"(C) the nature of that action or penalty; and

"(D) such other matters as the Secretary considers relevant and appropriate to provide full and complete information with respect to his activities under this subchapter.

"§ 7175. Judicial review

"(a) An employee, or applicant for employment, aggrieved by a final determination or order of the Board on Employee Rights may file, within 30 days after the date of that determination or order, in the district court of the United States for the judicial district in which the alleged violation or threatened violation of section 7173(a) of this title occurred or in which his official duty station was located at the time of the alleged violation or threatened violation—

"(1) a petition for a review of the determination or order; or

"(2) a complaint for a trial de novo on the violation or threatened violation of section 7173(a) of this title, which was the subject of the determination or order of the Board.

The petition or complaint shall name as defendant both the Executive agency concerned and the Board on Employee Rights. An official, or former official, of an Executive agency—

"(A) with respect to whom, in connection with the

petition for review, there is involved an alleged violation or threatened violation by him of section 7173 (a) of this title;

"(B) with respect to whom the complaint for a trial de novo, or the trial pursuant to the complaint, involves an alleged violation or threatened violation by him of section 7173 (a) of this title; or

"(C) aggrieved by a final determination or order of the Board, or part or application thereof, in connection with such alleged violation or threatened violation;

is entitled, in his individual capacity, to file an answer with respect to such violation or threatened violation and participate as a party in the proceedings.

"(b) If, after the expiration of 30 days after the date of a final determination or order of the Board, a petition or complaint with respect to such determination or order has not been filed under subsection (a) of this section, an official or former official of an Executive agency aggrieved by that determination or order, or part or application thereof, may file, within 30 days after the expiration of such 30-day period, in the district court of the United States for the judicial district in which the alleged violation or threatened violation of section 7173 (a) of this title occurred or in which his official duty station was located at the time of the alleged

violation or threatened violation, a petition for review of the determination or order, or part or application thereof.

"(c) A petition for review or complaint for trial de novo filed under subsection (a) or (b) of this section shall name as defendant both the Executive agency concerned and the Board, and a copy thereof shall be served on the Executive agency concerned and the Board.

"(d) When a copy of a petition for review is served on the Board, a certified copy of the record on which the final determination or order of the Board is based shall be filed with the court. On filing of a petition with the court, and in its consideration of the petition, the court shall have jurisdiction to—

"(1) issue such restraining order, interlocutory injunction, permanent injunction, or mandatory injunction, as may be necessary and appropriate with respect to any determination or order, or part or application thereof, made by the Board which is under review;

"(2) affirm, modify, or set aside any such determination or order, or part or application thereof;

"(3) require the Board to make any determination or order which it is authorized to make under section 7174(j) of this title, but which it has failed or refused to make; and

"(4) remand the matter to the Board for appropri-

ate action by the Board and the Executive agency concerned in accordance with the decision of the court. The reviewing court shall set aside any finding, conclusion, determination, or order of the Board as to which a complaint is made that is unsupported by substantial evidence on the record considered as a whole.

"(e) On the filing of a complaint for a trial de novo, the court shall have jurisdiction to—

"(1) try and determine the action, irrespective of the existence or amount of pecuniary injury done or threatened; and

"(2) issue such restraining order, interlocutory injunction, permanent injunction, or mandatory injunction, or enter such other judgment or decree, as may be necessary or appropriate to prevent the threatened violation or to afford the plaintiff and others similarly situated complete relief against the consequences of any violation. The court shall decide all questions of law in any action under this subsection. The court, upon application by either party, shall order a trial by jury of the issues in any action under this subsection.

"(f) With the written consent, filed with the court, of an employee, applicant for employment, official of an Executive agency, or former official of an Executive agency aggrieved by a final determination or order of the Board, who

is entitled to file a petition for review, a complaint for a trial de novo, or answer, or to participate as a party in any proceeding, under this section, not more than one labor organization, or association of supervisors, representing employees may intervene in connection with the review or the trial de novo.

"§ 7176. General provisions

"(a) An individual called on to participate in any phase of an administrative or judicial proceeding under this subchapter shall be free from restraint, coercion, interference, intimidation, or reprisal in the course of, or because of, his participation.

"(b) An employee or an official of an Executive agency who is a party to the action, summoned, or assigned by his agency to appear, including an appearance to give his deposition, before the Board on Employee Rights, or before the appropriate court, in connection with any matter before the Board or the court under this subchapter, shall not incur a loss of or reduction in any right, entitlement, or benefit as an employee or official of that agency. A period of such absence within his regularly scheduled tour of duty is service performed by the employee or official while on official business. Travel by the employee or official during a period of such absence, whether or not performed within his regularly scheduled tour of duty, is travel on official business.

"(c) On written application certifying his expenses and charges filed with the Board on Employee Rights by an attorney representing a party to the action who has appeared before the Board, or the appropriate court, in connection with any matter before the Board, or the court, or both, under this subchapter, which has been determined by the Board or the court, in favor of the party represented by the attorney, the Board may allow, at the conclusion of the representation and in accordance with the regulations prescribed under section 7174(c) of this title, such remuneration to the attorney as it considers reasonable and proper and shall certify to the Executive agency concerned the amount of the attorney's remuneration granted by it. The agency shall pay the certified amount of such remuneration, in accordance with the following provisions:

"(1) the agency shall charge against such certified amount of remuneration all sums previously paid to the attorney by the party represented;

"(2) if the sums previously paid to the attorney by that party for such representation equal or exceed the certified amount of the attorney's remuneration, the agency shall reimburse that party in that certified amount; and

"(3) if the sums previously paid to the attorney by that party for such representation are less than that

certified amount, the agency shall reimburse that party in the amount paid by that party and shall pay to the attorney an amount equal to the difference between the certified amount of the attorney's remuneration and the aggregate of the sums previously paid by that party to the attorney.".

(b) The analysis of chapter 71 of title 5, United States Code, is amended by adding the following at the end thereof:

"SUBCHAPTER III—EMPLOYEE RIGHTS

"Sec.
"7171. Policy.
"7172. Definition.
"7173. Employee rights.
"7174. Board on Employee Rights.
"7175. Judicial review.
"7176. General provisions.".

(c) Section 5316 of title 5, United States Code, is amended by adding at the end thereof:

"(131) Members of the Board on Employee Rights (3).".

SEC. 2. Subchapter III of chapter 71 of title 5, United States Code, as added by this Act, shall apply only with respect to acts, violations, threatened violations, grievances, and other similar matters covered by such subchapter which arise or occur on or after such date following the date of enactment of this Act as the Board on Employee Rights, established by the amendments made by the first section of this Act, shall prescribe but in no event later than the

one hundred and eightieth day following such date of enactment.

SEC. 3. Notwithstanding section 7174 of title 5, United States Code, as added by the first section of this Act, the terms of office of the three members first appointed to the Board on Employee Rights shall end, as designated by the President, one at the end of 2 years, one at the end of 4 years, and one at the end of 6 years.

93D CONGRESS
1ST SESSION

H. R. 7677

IN THE HOUSE OF REPRESENTATIVES

MAY 9, 1973

Mr. FRENZEL introduced the following bill; which was referred to the Committee on Post Office and Civil Service

A BILL

To protect the civilian employees of the executive branch of the United States Government in the enjoyment of their constitutional rights and to prevent unwarranted governmental invasions of their privacy.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. It shall be unlawful for any officer of any executive department or any executive agency of the United States Government, or for any person acting or purporting to act under his authority, to do any of the following things:

(a) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency, or any person seeking employment in the executive branch of the United States Government, to disclose his race, religion, or national origin, or the race, religion, or national origin of any of his forebears: *Provided, however,* That nothing contained in this subsection shall be construed to prohibit inquiry concerning the citizenship of any such employee or person if his citizenship is a statutory condition of his obtaining or retaining his employment: *Provided further,* That nothing contained in this subsection shall be construed to prohibit inquiry concerning the national origin or citizenship of any such employee or person or of his forebears, when such inquiry is deemed necessary or advisable to determine suitability for assignment to activities or undertakings related to the national security within the United States or to activities or undertakings of any nature outside the United States.

(b) To state or intimate, or to attempt to state or intimate, to any civilian employee of the United States serving in the department or agency that any notice will be taken of his attendance or lack of attendance at any assemblage, discussion, or lecture held or called by any officer of the executive branch of the United States Government, or by any person acting or purporting to act under his authority, or by any

outside parties or organizations to advise, instruct, or indoctrinate any civilian employee of the United States serving in the department or agency in respect to any matter or subject other than the performance of official duties to which he is or may be assigned in the department or agency, or the development of skills, knowledge, or abilities which qualify him for the performance of such duties: *Provided, however,* That nothing contained in this subsection shall be construed to prohibit taking notice of the participation of a civilian employee in the activities of any professional group or association.

(c) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to participate in any way in any activities or undertakings unless such activities or undertakings are related to the performance of official duties to which he is or may be assigned in the department or agency, or to the development of skills, knowledge, or abilities which qualify him for the performance of such duties.

(d) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to make any report concerning any of his activities or undertakings unless such activities or undertakings are related to the performance of official duties to which he is or may be assigned in the

department or agency, or to the development of skills, knowledge, or abilities which qualify him for the performance of such duties, or unless there is reason to believe that the civilian employee is engaged in outside activities or employment in conflict with his official duties.

(e) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency, or any person applying for employment as a civilian employee in the executive branch of the United States Government, to submit to any interrogation or examination or to take any psychological test which is designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters: *Provided, however,* That nothing contained in this subsection shall be construed to prevent a physician from eliciting such information or authorizing such tests in the diagnosis or treatment of any civilian employee or applicant where such physician deems such information necessary to enable him to determine whether or not such individual is suffering from mental illness: *Provided further, however,* That this determination shall be made in individual cases and not pursuant to general practice or regulation governing the examination of employees or

applicants according to grade, agency, or duties: *Provided further, however,* That nothing contained in this subsection shall be construed to prohibit an officer of the department or agency from advising any civilian employee or applicant of a specific charge of sexual misconduct made against that person, and affording him an opportunity to refute the charge.

(f) To require or request, or attempt to require or request, any civilian employee of the United States serving in the department or agency, or any person applying for employment as a civilian employee in the executive branch of the United States Government, to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

(g) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to support by personal endeavor or contribution of money or any other thing of value the nomination or the election of any person or group of persons to public office in the Government of the United States or of any State, district, Commonwealth, territory, or possession of the United States, or to attend any meeting held to promote or support the activities or undertakings of any political

party of the United States or of any State, district, Commonwealth, territory, or possession of the United States.

(h) To coerce or attempt to coerce any civilian employee of the United States serving in the department or agency to invest his earnings in bonds or other obligations or securities issued by the United States or any of its departments or agencies, or to make donations to any institution or cause of any kind: *Provided, however,* That nothing contained in this subsection shall be construed to prohibit any officer of any executive department or any executive agency of the United States Government, or any person acting or purporting to act under his authority, from calling meetings and taking any action appropriate to afford any civilian employee of the United States the opportunity voluntarily to invest his earnings in bonds or other obligations or securities issued by the United States or any of its departments or agencies, or voluntarily to make donations to any institution or cause.

(i) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency to disclose any items of his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family or household: *Provided, however,* That this subsection shall not apply to any civilian

employee who has authority to make any final determination with respect to the tax or other liability of any person, corporation, or other legal entity to the United States, or claims which require expenditure of moneys of the United States: *Provided further, however,* That nothing contained in this subsection shall prohibit the Department of the Treasury or any other executive department or agency of the United States Government from requiring any civilian employee of the United States to make such reports as may be necessary or appropriate for the determination of his liability for taxes, tariffs, custom duties, or other obligations imposed by law.

(j) To require or request, or to attempt to require or request, any civilian employee of the United States embraced within the terms of the proviso in subsection (i) to disclose any items of his property, income, or other assets, source of income, or liabilities, or his personal or domestic expenditures or those of any member of his family or household other than specific items tending to indicate a conflict of interest in respect to the performance of any of the official duties to which he is or may be assigned.

(k) To require or request, or to attempt to require or request, any civilian employee of the United States serving in the department or agency, who is under investigation for

misconduct, to submit to interrogation which could lead to disciplinary action without the presence of counsel or other person of his choice, if he so requests: *Provided, however,* That a civilian employee of the United States serving in the Central Intelligence Agency or the National Security Agency may be accompanied only by a person of his choice who serves in the agency in which the employee serves, or by counsel who has been approved by the agency for access to the information involved.

(l) To discharge, discipline, demote, deny promotion to, relocate, reassign, or otherwise discriminate in regard to any term or condition of employment of, any civilian employee of the United States serving in the department or agency, or to threaten to commit any of such acts, by reason of the refusal or failure of such employee to submit to or comply with any requirement, request, or action made unlawful by this Act, or by reason of the exercise by such civilian employee of any right granted or secured by this Act.

SEC. 2. It shall be unlawful for any officer of the United States Civil Service Commission, or for any person acting or purporting to act under his authority, to do any of the following things:

(a) To require or request, or to attempt to require or request, any executive department or any executive agency

of the United States Government, or any officer or employee serving in such department or agency, to violate any of the provisions of section 1 of this Act.

(b) To require or request, or to attempt to require or request, any person seeking to establish civil service status or eligibility for employment in the executive branch of the United States Government, or any person applying for employment in the executive branch of the United States Government, or any civilian employee of the United States serving in any department or agency of the United States Government, to submit to any interrogation or examination or to take any psychological test which is desgined to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters: *Provided, however,* That nothing contained in this subsection shall be construed to prevent a physician from eliciting such information or authorizing such tests in the diagnosis or treatment of any civilian employee or applicant where such physician deems such information necessary to enable him to determine whether or not such individual is suffering from mental illness: *Provided further, however,* That this determination shall be made in individual cases and not pursuant to general practice or regulation governing the exami-

nation of employees or applicants according to grade, agency, or duties: *Provided, further, however,* That nothing contained in this subsection shall be construed to prohibit an officer of the Civil Service Commission from advising any civilian employee or applicant on a specific charge of sexual misconduct made against that person, and affording him an opportunity to refute the charge.

(c) To require or request, or to attempt to require or request, any person seeking to establish civil service status or eligibility for employment in the executive branch of the United States Government, or any person applying for employment in the executive branch of the United States Government, or any civilian employee of the United States serving in any department or agency of the United States Goverment, to take any polygraph test designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters.

SEC. 3. It shall be unlawful for any commissioned officer, as defined in section 101 of title 10, United States Code, or any member of the Armed Forces acting or purporting to act under his authority, to require or request, or to attempt to require or request, any civilian employee of the executive branch of the United States Government under his authority

or subject to his supervision to perform any of the acts or submit to any of the requirements made unlawful by section 1 of this Act.

SEC. 4. Whenever any officer of any executive department or any executive agency of the United States Government, or any person acting or purporting to act under his authority, or any commissioned officer as defined in section 101 of title 10, United States Code, or any member of the Armed Forces acting or purporting to act under his authority, violates or threatens to violate any of the provisions of section 1, 2, or 3 of this Act, any civilian employee of the United States serving in any department or agency of the United States Government, or any person applying for employment in the executive branch of the United States Government, or any person seeking to establish civil service status or eligibility for employment in the executive branch of the United States Government, affected or aggrieved by the violation or threatened violation, may bring a civil action in his own behalf or in behalf of himself and others similarly situated, against the offending officer or person in the United States district court for the district in which the violation occurs or is threatened, or the district in which the offending officer or person is found, or in the United States District Court for the District of Columbia, to prevent the threatened violation or to obtain redress against the

consequences of the violation. The Attorney General shall defend all officers or persons sued under this section who acted pursuant to an order, regulation, or directive, or who, in his opinion, did not willfully violate the provisions of this Act. Such United States district court shall have jurisdiction to try and determine such civil action irrespective of the actuality or amount of pecuniary injury done or threatened, and without regard to whether the aggrieved party shall have exhausted any administrative remedies that may be provided by law, and to issue such restraining order, interlocutory injunction, permanent injunction, or mandatory injunction, or enter such other judgment or decree as may be necessary or appropriate to prevent the threatened violation, or to afford the plaintiff and others similarly situated complete relief against the consequences of the violation. With the written consent of any person affected or aggrieved by a violation or threatened violation of section 1, 2, or 3 of this Act, any employee organization may bring such action on behalf of such person, or may intervene in such action. For the purposes of this section, employee organizations shall be construed to include any brotherhood, council, federation, organization, union, or professional association made up in whole or in part of civilian employees of the United States and which has as one of its purposes dealing with departments, agencies, commissions,

and independent agencies of the United States concerning the condition and terms of employment of such employees.

SEC. 5. (a) There is hereby established a Board on Employees' Rights (hereinafter referred to as the "Board"). The Board shall be composed of three members, appointed by the President, by and with the advice and consent of the Senate. The President shall designate one member as chairman. No more than two members of the Board may be of the same political party. No member of the Board shall be an officer or employee of the United States Government.

(b) The term of office of each member of the Board shall be five years, except that (1) of those members first appointed, one shall serve for five years, one for three years, and one for one year, respectively, from the date of enactment of this Act, and (2) any member appointed to fill a vacancy occurring prior to the expiration of the term for which his predecessor was appointed shall be appointed for the remainder of such term.

(c) Members of the Board shall be compensated at the rate of $75 a day for each day spent in the work of the Board, and shall be paid actual travel expenses and per diem in lieu of subsistence expenses when away from their usual places of residence, as authorized by section 5703 of title 5, United States Code.

(d) Two members shall constitute a quorum for the transaction of business.

(e) The Board may appoint and fix the compensation of such officers, attorneys, and employees, and make such expenditures, as may be necessary to carry out its functions.

(f) The Board shall make such rules and regulations as shall be necessary and proper to carry out its functions.

(g) The Board shall have the authority and duty to receive and investigate written complaints from or on behalf of any person claiming to be affected or aggrieved by any violation or threatened violation of this Act and to conduct a hearing on each such complaint. Within ten days after the receipt of any such complaint, the Board shall furnish notice of the time, place, and nature of the hearing thereon to all interested parties. The Board shall render its final decision with respect to any complaint within thirty days after the conclusion of its hearing thereon.

(h) Officers or representatives of any Federal employee organization in any degree concerned with employment of the category in which any alleged violation of this Act occurred or is threatened shall be given an opportunity to participate in each hearing conducted under this section, through submission of written data, views, or arguments, and in the discretion of the Board, with opportunity for oral presentation. Government employees called upon by any

party or by any Federal employee organization to participate in any phase of any administrative or judicial proceeding under this section shall be free to do so without incurring travel cost or suffering loss in leave or pay; and all such employees shall be free from restraint, coercion, interference, intimidation, or reprisal in or because of their participation. Any periods of time spent by Government employees during such participation shall be held and considered to be Federal employment for all purposes.

(i) Insofar as consistent with the purposes of this section, the provisions of subchapter II of chapter 5 of title 5, United States Code, relating to the furnishing of notice and manner of conducting agency hearings, shall be applicable to hearings conducted by the Board under this section.

(j) If the Board shall determine after hearing that a violation of this Act has not occurred or is not threatened, the Board shall state its determination and notify all interested parties of such determination. Each such determination shall constitute a final decision of the Board for purposes of judicial review.

(k) If the Board shall determine that any violation of this Act has been committed or threatened by any civilian officer or employee of the United States, the Board shall immediately (1) issue and cause to be served on such officer or employee an order requiring such officer or employee

to cease and desist from the unlawful act or practice which constitutes a violation, (2) endeavor to eliminate any such unlawful act or practice by informal methods of conference, conciliation, and persuasion, and (3) may—

(A) (i) in the case of the first offense by any civilian officer or employee of the United States, other than any officer appointed by the President, by and with the advice and consent of the Senate, issue an official reprimand against such officer or employee or order the suspension without pay of such officer or employee from the position or office held by him for a period of not to exceed fifteen days, and (ii) in the case of a second or subsequent offense by any such officer or employee, order the suspension without pay of such officer or employee from the position or office held by him for a period of not to exceed thirty days or order the removal of such officer or employee from such position or office; and

(B) in the case of any offense by any officer appointed by the President, by and with the advice and consent of the Senate, transmit a report concerning such violation to the President and the Congress.

(l) If the Board shall determine that any violation of this Act has been committed or threatened by any officer of any of the Armed Forces of the United States, or any

person purporting to act under authority conferred by such officer, the Board shall (1) submit a report thereon to the President, the Congress, and the Secretary of the military department concerned, (2) endeavor to eliminate any unlawful act or practice which constitutes such a violation by informal methods of conference, conciliation, and persuasion, and (3) refer its determination and the record in the case to any person authorized to convene general courts-martial under section 822 (article 22) of title 10, United States Code. Thereupon such person shall take immediate steps to dispose of the matter under chapter 47 of title 10, United States Code (Uniform Code of Military Justice).

(m) Any party aggrieved by any final determination or order of the Board may institute, in the district court of the United States for the judicial district wherein the violation or threatened violation of this Act occurred, or in the United States District Court for the District of Columbia, a civil action for the review of such determination or order. In any such action, the court shall have jurisdiction to (1) affirm, modify, or set aside any determination or order made by the Board which is under review, or (2) require the Board to make any determination or order which it is authorized to make under subsection (k), but which it has refused to make. The reviewing court shall set aside any finding, conclusion, determination, or order of the Board as to which

complaint is made which is unsupported by substantial evidence on the record considered as a whole.

(n) The Board shall submit, not later than March 31 of each year, to the Senate and House of Representatives, respectively, a report on its activities under this section during the immediately preceding calendar year, including a statement concerning the nature of all complaints filed with it, its determinations and orders resulting from hearings thereon, and the names of all officers or employees of the United States with respect to whom any penalties have been imposed under this section.

(o) There are authorized to be appropriated sums necessary, not in excess of $100,000, to carry out the provisions of this section.

SEC. 6. Nothing contained in this Act shall be construed to prohibit an officer of the Central Intelligence Agency or of the National Security Agency from requesting any civilian employee or applicant to take a polygraph test, or to take a psychological test, designed to elicit from him information concerning his personal relationship with any person connected with him by blood or marriage, or concerning his religious beliefs or practices, or concerning his attitude or conduct with respect to sexual matters, or to provide a personal financial statement, if the Director of the Central Intelligence Agency or his designee or the Director of the National Security Agency or his designee makes a personal

finding with regard to each individual to be so tested or examined that such test or information is required to protect the national security.

SEC. 7. No civilian employee of the United States serving in the Central Intelligence Agency or the National Security Agency, and no individual or organization acting in behalf of such employee, shall be permitted to invoke the provisions of sections 4 and 5 without first submitting a written complaint to the agency concerned about the threatened or actual violation of this Act and affording such agency one hundred and twenty days from the date of such complaint to prevent the threatened violation or to redress the actual violation: *Provided, however,* That nothing in this Act shall be construed to affect any existing authority of the Director of Central Intelligence under section 403 (c), of title 50, United States Code, and any authorities available to the National Security Agency under section 833 of title 50, United States Code, to terminate the employment of any employee.

SEC. 8. Nothing in this Act shall be construed to affect in any way the authority of the Directors of the Central Intelligence Agency or the National Security Agency to protect or withhold information pursuant to statute or executive order. The personal certification by the Director of the agency that disclosure of any information is inconsistent with the provision of any statute or Executive order shall be conclusive and no such information shall be admissible in evi-

dence in any interrogation under section 1 (k) or in any civil action under section 4 or in any proceeding or civil action under section 5.

SEC. 9. This Act shall not be applicable to the Federal Bureau of Investigation.

SEC. 10. Nothing contained in sections 4 and 5 shall be construed to prevent establishment of department and agency grievance procedures to enforce this Act, but the existence of such procedures shall not preclude any applicant or employee from pursuing the remedies established by this Act or any other remedies provided by law: *Provided, however*, That if under the procedures established, the employee or applicant has obtained complete protection against threatened violations or complete redress for violations, such action may be pleaded in bar in the United States district court or in proceedings before the Board on Employee Rights: *And provided further*, That if an employee elects to seek a remedy under either section 4 or section 5, he waives his right to proceed by an independent action under the remaining section.

SEC. 11. If any provision of this Act or the application of any provision to any person or circumstance shall be held invalid, the remainder of this Act or the application of such provision to persons or circumstances other than those as to which it is held invalid, shall not be affected.

93D CONGRESS
2D SESSION

H. R. 12206

IN THE HOUSE OF REPRESENTATIVES

JANUARY 22, 1974

Mr. KOCH introduced the following bill; which was referred to the Committee on Government Operations

A BILL

To amend title 5, United States Code, to provide that persons be apprised of records concerning them which are maintained by Government agencies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That (a) title 5, United States Code, is amended by adding immediately after section 552 thereof the following new section:

"§ 552a. Individual records

"(a) Each agency that maintains records, including computer records, concerning any person which may be retrieved by reference to, or are indexed under such person's name, or some other similar identifying number or

symbol, and which contain any information obtained from any source other than such person shall, with respect to such records—

"(1) refrain from disclosing the record or any information contained therein to any other agency or to any person not employed by the agency maintaining such record, except—

"(A) with notification of the person concerned or, in the event such person, if an individual, cannot be located or communicated with after reasonable effort, with notification of members of the individual's immediate family or guardian, or, only in the event that such individual, members of the individual's immediate family, and guardian cannot be located or communicated with after reasonable effort, upon good cause for such disclosure, or

"(B) that if disclosure of such record is required under section 552 of this chapter or by any other provision of law, the person concerned shall be notified by mail at his last known address of any such required disclosure;

"(2) refrain from disclosing the record or any information contained therein to individuals within that formation contained therein to individuals within that agency other than those individuals who need to ex-

amine such record or information for the execution of their jobs;

"(3) maintain an accurate record of the names and addresses of all persons to whom any information contained in such records is divulged and the purposes for which such divulgence was made;

"(4) permit any person to inspect his own record and have copies thereof made at his expense, which in no event shall be greater than the cost to the agency of making such copies;

"(5) permit any person to supplement the information contained in his record by the addition of any document or writing of reasonable length containing information such person deems pertinent to his record; and

"(6) remove erroneous information of any kind, and notify all agencies and persons to whom the erroneous material has been previously transferred of its removal.

"(b) This section shall not apply to records that are—

"(1) specifically required by Executive order to be kept secret in the interest of the national defense and foreign policy;

"(2) investigatory files compiled for law enforcement purposes, except to the extent that such records have been maintained for a longer period than reason-

ably necessary to commence prosecution or other action or to the extent available by law to a party other than an agency.

"(c) The President shall report to Congress before January 30 of each year on an agency-by-agency basis the number of records and the number of investigatory files which were exempted from the application of this section by reason of clauses (1) and (2) of subsection (d) during the immediately preceding calendar year.

"(d) This section shall not be held or considered to permit the disclosure of the identity of any person who has furnished information contained in any record subject to this section.

"(e) Each agency that maintains records subject to the provisions of this section shall publish rules establishing reasonable times, places, fees to the extent authorized, and procedures to be followed with respect to making records promptly available to an individual and otherwise to implement the provisions of section 552a of title 5 of the United States Code.

"(f) Any employee of the United States who under the color of agency authority knowingly and willfully violates a provision of this section, or permits such a violation, shall be fined $1,000.

"(g) Nothing in this section shall be construed to permit transfer or similar distribution of any information deemed confidential by other statutes.".

(b) The table of sections of chapter 5 of title 5, United States Code, is amended by inserting:

"552a. Individual records."

immediately below:

"552. Public information; agency rules; opinions, orders, records, and proceedings.".

SEC. 2. The amendments made by this Act shall become effective on the ninetieth day following the date of enactment of this Act.

63-619 O - 76 - 47

93D CONGRESS
2D SESSION

H. R. 13872

IN THE HOUSE OF REPRESENTATIVES

APRIL 2, 1974

Ms. ABZUG introduced the following bill; which was referred to the Committee on Government Operations

A BILL

To amend title 5, United States Code, to provide for the privacy of individual's records maintained by Federal agencies.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That (a) the Congress finds—

(1) that an individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record;

(2) that a record containing information about an individual in identifiable form must be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be,

and what disclosure and use will be made of the identifiable information in it; and

(3) that any recording, disclosure, and use of identifiable personal information by an agency not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure, or use is specifically authorized by Federal statute.

(b) The purpose of this Act is to insure safeguards for personal privacy from Federal agencies by adherence to the following principles of information practice:

(1) There must be no personal data recordkeeping system whose very existence is secret.

(2) There must be a way for an individual to find out what information about him is in a record and how it is used.

(3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

(4) There must be a way for an individual to correct or amend a record of identifiable information about him.

(5) Any agency creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use

and must take reasonable precautions to prevent misuse of the data.

(6) Deviations from these principles should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount governmental interest can be clearly demonstrated. No deviation should be permitted except as specifically provided by statute.

SEC. 2. (a) Subchapter II of chapter 5 of title 5, United States Code, is amended by adding at the end thereof the following new sections:

"§ 552a. Individual records

"(a) For purposes of this subsection, the term—

"(1) 'records' means computer-accessible or manual-accessible information or portions thereof containing personal data that can be associated with identifiable individuals; or that affords a clear basis for inferring personal characteristic or things done by or to an individual, such as the mere record of his presence in a place, attendance at a meeting, or admissions to some type of service institution;

"(2) 'data subject' means the individual whose name or identity is added to or maintained on an automated or manual personal data system;

"(3) 'notification' means communication to the

data subject of (A) the date of the disclosure; (B) the content of the records to be disclosed; (C) the agency or person to whom the records shall be disclosed; and (D) the purpose for which the disclosure is being effected;

"(4) 'consent' means an authorization signed by the data subject for a specific agency or person to use specific records for a specific purpose, and shall be obtained by notification to the data subject by registered mail, return receipt requested;

"(5) 'constructive consent' means notification to the data subject by registered mail, return receipt requested, with proof of receipt but failure of the data subject to respond or object within fourteen days after date of receipt;

"(6) 'disclosure' means the transmission of records or portions thereof, whether orally, by writing or by wire;

"(7) 'unfair information practice' means a failure to comply with any safeguard requirements of this Act.

"(b) Each agency that maintains records shall—

"(1) refrain from disclosing the record or any information contained therein to any other Federal, State,

or local agency or to any person not employed by the agency maintaining such record, except—

"(A) with consent or constructive consent of the individual concerned or, in the event such individual cannot be located or communicated with after reasonable effort, with permission from members of the individual's immediate family, guardian, or, only in the event that such individual, members of the individual's immediate family, and guardian cannot be located or communicated with after reasonable effort, upon good cause for such disclosure, or

"(B) that if disclosure of such record is required under this section of this chapter or by any other provision of law, including by means of compulsory legal process, the individual concerned shall be notified by mail at his last known address of any such required disclosure; and shall be afforded full access to the records at least ten days before they are made available in response to the demand;

"(2) refrain from disclosing the records to any individuals within that agency other than those individuals who need to examine such records in the performance of their duties;

"(3) maintain an accurate register which shall become part of the individual's record, of the names and job classifications of all persons to whom such records are disclosed and the purposes for which such disclosure was made;

"(4) permit any data subject to inspect his own record upon proper identification at a convenient local office or by mail, or by telephone, and have copies thereof made at his expense, which in no event shall be greater than the cost of reproduction;

"(5) permit any data subject to supplement the information contained in his record by the addition of any document or writing or photograph containing information such individual deems pertinent to his record, and notify all agencies and persons to whom the records were previously disclosed of the supplemental information;

"(6) remove from records and promptly destroy all erroneous or irrelevant information and notify all agencies or persons to whom such information has been previously transferred of its removal and the reason for its removal; and in case of dispute as to what constitutes erroneous or irrelevant information, the issue shall be determined by the Federal Privacy Board;

"(7) upon written request of any data subject, give

notice to such individual, in the event that his record has been augmented, of the contents of the augmentation, the source of the augmentation, and the purpose for which the augmentation is being effected;

"(8) inform an individual asked to supply personal data for any agency recordkeeping system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the agency, of providing or not providing such data; and

"(9) assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless, in the case of each use of such data, the informed consent of the individual has been explicitly obtained.

"(c) Subparagraphs (1), (4), and (7) of paragraph (b) shall not apply to records that have been opened and are being used in the pursuit of an active criminal prosecution, except to the extent that such records have been maintained for a longer period than is reasonably necessary to commence prosecution or to the extent available by law to a party other than an agency.

"(d) Subparagraphs (1), (4), and (7) of paragraph (b) shall not apply to records authorized under criteria es-

tablished by an Executive order to be kept secret in the interest of national defense or foreign policy and the disclosure of which would—

"(1) endanger the active military plans or deployment of United States forces,

"(2) reveal details about current military technology or weaponry, or

"(3) endanger the life of any person engaged in foreign intelligence gathering operations of the United States Government.

"(e) The President shall report to Congress before January 30 of each year on an agency-by-agency basis the number of records which were exempted from the application of this section by reason of paragraph (c) or (d) during the immediately preceding calendar year.

"(f) Any person who under the color of agency authority willingly or knowingly permits or causes to occur an unfair information practice shall be fined not more than $10,000 or imprisoned for not more than one year or suspended from employment without pay for not more than one year, or any combination thereof.

"(g) Any person or agency which commits an unfair information practice shall be liable in an amount equal to—

"(1) actual and general damages but not less than

liquidated damages computed at the rate of $1,000 for each unfair information practice:

"(2) exemplary and punitive damages; and

"(3) reasonable attorney's fees and other litigation costs reasonably incurred.

"(h) Any individual who has reason to believe that his records have been, are being, or are about to be disclosed in violation of paragraph (b) may bring an action in the appropriate district court of the United States to enjoin such disclosure, and upon a proper showing a temporary restraining order or a preliminary or permanent injunction shall be granted without bond.

"(i) An action to enforce any liability created under this section may be brought in any appropriate United States district court without regard to the amount in controversy within two years from the date on which the liability arises, except where a defendant has materially and willfully failed to comply with the safeguards under this section, the action may be brought at any time within two years after discovery by the individual data subject.

"§ 552b. Federal Privacy Board

"(a) There is hereby established a Board to be known as the Federal Privacy Board (hereinafter referred to as the 'Board').

"(b) The Board shall consist of seven members, each serving for a term of two years, four of whom shall constitute a quorum. The members of the Board shall be appointed by the President, by and with the advice and consent of the Senate. No more than four of the members appointed shall be of the same political party, and shall be from the public at large and not officers or employees of the United States. Any vacancy in the Board shall be filled in the same manner as the original appointment was made.

"(c) Members of the Board shall be entitled to receive $100 each day during which they are engaged in the performance of the business of the Board, including traveltime.

"(d) The Chairman of the Board shall be elected by the Board every year, and the Board shall meet not less frequently than bimonthly.

"(e) The Board shall appoint and fix the compensation of such personnel as are necessary to the carrying out of its duties.

"(f) The Board shall establish published rules stating the time, place, fees to the extent authorized, and procedures to be followed with respect to making records promptly available to data subjects, and otherwise to implement the provisions of section 552a of title 5 of the United States Code.

"(g) The Board shall periodically publish and dis-

tribute through local post offices a Citizen's Privacy Index which shall include—

"(1) the name and location of every agency data keeping system;

"(2) the title, name, and address of the person immediately responsible for the system;

"(3) the nature and purpose of the system;

"(4) the categories and number of persons on whom data are maintained;

"(5) the categories of data maintained, indicating which categories are stored in computer-accessible files and which data are stored in manual-accessible files;

"(6) each agency's policies and practices regarding data storage, duration of retention of data, and disposal thereof;

"(7) the categories of data sources;

"(8) a description of all types of use made of data, including all classes of users and the agency relationships among them; and

"(9) the procedures whereby an individual can (A) be informed if he is the subject of data in the systems; (B) gain access to such data; and (C) contest their accuracy, completeness, timeliness, pertinence, and the necessity for retaining such data.

"(h) The Board shall devise and distribute printed request forms, preaddressed to agencies to enable individuals to exercise the rights granted pursuant to section 552a (b) (4) and (7) of title 5 of the United States Code.

"(i) The Board shall provide trained personnel to assist individuals upon request in interpreting their records.

"(j) The Board shall promptly consider complaints from any person that one or more of the requirements of section 552a of title 5, United States Code, has not been met, with respect to the records specified in such section, by the responsible agency. The Board, upon finding that one or more of the requirements has not been met, shall issue a final order directing the agency to comply with such requirement or requirements, and this order shall be binding on the parties to such a dispute.

"(k) The Board shall hold hearings in order to make findings upon each complaint, unless it determines that the complaint is frivolous. The Board may examine such evidence as it deems useful, and shall establish such rules and procedures as it determines are most apt to the purposes of this section, including rules insuring the exhaustion of administrative remedies in the appropriate agency.

"(l) The Board shall establish a program to educate the public with respect to the provisions of section 552a of title 5, United States Code."

(b) The table of sections of subchapter II of chapter 5 of title 5, United States Code, is amended by inserting after the heading for section 552 the following new headings:

"552a. Individual records.
"552b. Federal Privacy Board."

SEC. 3. The amendments made by this Act shall become effective upon the expiration of the ninety-day period which begins on the date of the enactment of this Act.

93D CONGRESS
2D SESSION

H. R. 14493

IN THE HOUSE OF REPRESENTATIVES

APRIL 30, 1974

Mr. GOLDWATER (for himself and Mr. KOCH) introduced the following bill; which was referred to the Committee on Government Operations

A BILL

To protect the right of privacy of individuals concerning whom identifiable information is recorded by the Federal Government by enacting principles to govern Federal agency information practices.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That chapter 5 of title 5, United States Code, is amended by adding immediately after section 552 thereof the following new title:

"SHORT TITLE

"SECTION 1. This title may be cited as the 'Right to Privacy Act'.

"FINDINGS AND DECLARATION OF POLICY

"SEC. 2. (a) The Congress finds—

"(1) that an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;

"(2) that the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

"(3) that an individual's opportunities to secure employment, insurance, credit and his right to due process, and other legal protections are endangered by these personal information system; and

"(4) that in order to preserve the rights guaranteed by the first, third, fourth, fifth, ninth, and fourteenth amendments of the United States Constitution, uniform Federal legislation is necessary to establish procedures to govern information systems containing records on individuals.

"(b) The purpose of this Act is to insure safeguards for personal privacy from Federal agencies by adherence to the following principles of information practice:

"(1) There should be no personal information system whose existence is secret.

"(2) Information should not be collected unless the need for it has been clearly established in advance.

"(3) Information should be appropriate and relevant to the purpose for which it has been collected.

"(4) Information should not be obtained by fraudulent or unfair means.

"(5) Information should not be used unless it is accurate and current.

"(6) There should be a prescribed procedure for an individual to learn the information stored about him, the purpose for which it has been recorded, and particulars about its use and dissemination.

"(7) There should be a clearly prescribed procedure for an individual to correct, erase, or amend inaccurate, obsolete, or irrelevant information.

"(8) Any Federal agency holding personal information should assure its reliability and take precautions to prevent its misuse.

"(9) There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent.

"(10) The Federal Government should not collect personal information except as authorized by law.

"DEFINITIONS

"SEC. 3. As used in this Act—

"(1) the term 'information system', means the

total components and operations of a recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars;

"(2) the term 'personal information' means all information that describes, locates, or indexes anything about an individual including his education, financial transactions, medical history, criminal, or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

"(3) the term 'data subject' means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system;

"(4) the term 'disseminate' means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means;

"(5) the term 'purge' means to obliterate information completely from the transient, permanent, or archival records of an organization; and

"(6) the term 'Federal agency' means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof.

"SAFEGUARD REQUIREMENTS FOR PERSONAL INFORMATION FOR ADMINISTRATIVE, STATISTICAL-REPORTING AND RESEARCH PURPOSES

"SEC. 4. (a) ADMINISTRATIVE REQUIREMENTS.—Any Federal agency maintaining an information system that includes personal information shall—

"(1) collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the agency;

"(2) collect information to the greatest extent possible from the data subject directly;

"(3) establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

"(4) maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

"(5) make no dissemination to another system without (A) specifying requirements for security and the use of information exclusively for the purposes set

forth in the notice—required under subsection (c) including limitations on access thereto, and (B) determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed;

"(6) transfer no personal information beyond the jurisdiction of the United States without specific authorization from the data subject or pursuant to a treaty or executive agreement in force guaranteeing that any foreign government or organization receiving personal information will comply with the applicable provisions of this Act with respect to that personal information;

"(7) afford any data subject of a foreign nationality, whether residing in the United States or not, the same rights under this Act as American citizens;

"(8) maintain a list of all persons having regular access to personal information in the information system;

"(9) maintain a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority;

"(10) take affirmative action to establish rules of conduct and inform each person involved in the design,

development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this Act, the rules and procedures of such agency, including penalties for noncompliance designed to assure compliance with such requirements;

"(11) establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;

"(12) shall collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used, or disseminated in or by any information system, unless authorized by statute.

"(b) SPECIAL ADDITIONAL REQUIREMENTS FOR STATISTICAL REPORTING AND RESEARCH INFORMATION SYSTEMS.—(1) Any Federal agency maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems or any non-Federal person or other Federal agency shall—

"(A) make available to any data subject or group, without revealing trade secrets, methodology and materials necessary to validate statistical analyses, and

"(B) make no materials available for independent analysis without guarantees that no personal information will be used in a way that might prejudice judgments about any data subject.

"(2) No Federal agency shall—

"(A) require any individual to disclose for statistical purposes any personal information unless such disclosure is required by a constitutional provision or act of Congress, and the individual is so informed;

"(B) request any individual voluntarily to disclose personal information unless such request has been specifically authorized by act of Congress, and the individual shall be advised that such disclosure is voluntary;

"(C) make available to any non-Federal person any statistical studies or reports or other compilations of information derived by mechanical or electronical means from files containing personal information, or no manual or computer material relating thereto, except those prepared, published, and made available for general public use; and

"(D) publish statistics of taxpayer income classified, in whole or in part, on the basis of a coding system for the delivery of mail.

"(3) Any Federal agency maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of any non-Federal person or other Federal agency, and which purges the names, personal numbers, or other identifying particulars of individuals and certifies to the Federal Privacy Board that no inferences may be drawn about any individual, shall be exempt from the requirements of sections 4 (a) (3), and (4), and sections 4 (c) and (d) (1), and (2).

"(c) PUBLIC NOTICE REQUIREMENT.—Any Federal agency maintaining or proposing to establish an information system for personal information shall—

"(1) give notice of the existence and character of each existing system once a year to the Federal Privacy Board;

"(2) give public notice of the existence and character of each existing system each year, in the Federal Register;

"(3) publish such annual notices for all its existing systems simultaneously; and

"(4) in the case of a new system, or the substantial modification of an existing system, shall give public notice and notice to the Federal Privacy Board within a reasonable time but in no case less than three months, in

advance of the initiation or modification to assure individuals who may be affected by its operation a reasonable opportunity to comment.

"(5) shall assure that public notice given under this subsection specifies the following:

"(A) The name of the system.

"(B) The general purpose of the system.

"(C) The categories of personal information, and approximate number of persons on whom information is maintained.

"(D) The categories of information maintained, confidentiality requirements, and access controls.

"(E) The Federal agency's policies and practices regarding information storage, duration of retention, and purging thereof.

"(F) The categories of information sources.

"(G) A description of types of use made of information including all classes of users and the organizational relationships among them.

"(H) The procedures whereby an individual can—

"(i) be informed if he is the subject of information in the system;

"(ii) gain access to such information; and

"(iii) contest the accuracy, completeness, timeliness, pertinence, and the necessity for retention.

"(I) The procedures whereby an individual or group can gain access to the information system used for statistical reporting or research in order to subject them to independent analysis.

"(J) The business address and telephone number of the person immediately responsible for the system.

"(d) RIGHTS OF DATA SUBJECTS.—Any Federal agency maintaining personal information shall—

"(1) inform an individual asked to supply personal information whether he is legally required, or may refuse, to supply the information requested, and also of any specific consequences which are known to the Federal agency, of providing or not providing such information;

"(2) request permission of a data subject to disseminate part or all of this information to another organization or system not having regular access authority, and indicate the use for which it is intended, and the specific consequences for the individual, which are known to the Federal agency, of providing or not providing such permission;

"(3) upon request and proper identification of any data subject, grant such subject the right to inspect, in a form comprehensible to such individual—

"(A) all personal information about that data subject except in the case of medical information, when such information shall, upon written authorization, be given to a physician designated by the data subject;

"(B) the nature of the sources of the information; and

"(C) the recipients of personal information about the data subject including the identity of all persons and Federal agencies involved and their relationship to the system when not having regular access authority.

"(4) comply with the following minimum conditions of disclosure to data subject:

"(A) A Federal agency shall make disclosures to data subjects required under this Act, during normal business hours.

"(B) The disclosures to data subjects required under this Act shall be made (i) in person, if he appears in person and furnishes proper identification, (ii) by mail, if he has made a written request,

with proper identification, at reasonable standard charges for document search and duplication.

"(C) The data subject shall be permitted to be accompanied by one person of his choosing, who must furnish reasonable identification. A Federal agency may require the data subject to furnish a written statement granting permission to the Federal agency to discuss that individual's file in such person's presence.

"(5) if the data subject gives notice that he wishes to challenge, correct, or explain information about him in the information system, the following minimum procedures shall be followed:

"(A) The Federal agency maintaining the information system shall investigate and record the current status of that personal information.

"(B) If, after such investigation, such information is found to be incomplete, inaccurate, not pertinent, not timely nor necessary to be retained, or can no longer be verified, it shall be promptly purged.

"(C) If the investigation does not resolve the dispute, the data subject may file a two hundred word statement setting forth his position

"(D) Whenever a statement of dispute is filed, the Federal agency maintaining the information system shall, in any subsequent dissemination or use of the information in question, clearly note that it is disputed and supply the statement of the data subject along with the information.

"(E) The Federal agency maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request.

"(F) Following any correction or purging of personal information the Federal agency shall at the request of the data subject, furnish to past recipients notification that the item has been purged or corrected.

"(G) In the case of a failure to resolve a dispute, the Federal agency shall advise the data subject of his right to request the assistance of the Federal Privacy Board.

"(e) NOTIFICATION PROCEDURE.—Data subjects of archival-type inactive files, records, or reports shall be notified by mail of the reactivation, accessing, or reaccessing not later than six months after the date of the enactment of this Act.

"EXEMPTIONS TO APPLICATIONS OF REQUIREMENTS

"SEC. 5. (a) The provisions of this Act shall not be applicable to personal information systems—

"(1) to the extent that information in such systems is maintained by a Federal agency, and the head of that agency determines that the release of the information would seriously damage national defense;

"(2) which are part of active criminal investigatory files compiled by Federal law enforcement organizations, except where such files have been maintained for a period longer than is necessary to commence criminal prosecution;

"(3) maintained by the press and news media, except information relating to employees of such organizations.

"(b) Any data subject denied access to personal information under this section shall be entitled to judicial review of the grounds for that denial in the appropriate United States district court.

"USE OF SOCIAL SECURITY NUMBER

"SEC. 6. It shall be unlawful for any Federal agency to require an individual to disclose or furnish his social security account number, for any purpose in connection with any activity, or to refuse to make a loan or to enter into any other transaction or relationship with an individual (except to the

extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program) wholly or partly because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by Federal law.

"FEDERAL PRIVACY BOARD

"SEC. 7. (a) ESTABLISHMENT.—There is established the Federal Privacy Board (hereinafter in this section referred to as the 'Board').

"(b) MEMBERSHIP.—The Board shall consist of five members, each serving for a term of three years, three of whom shall constitute a quorum. No member shall serve more than two terms. The members of the Board shall be appointed by the President, by and with the advice and consent of the Senate. No more than three of the members appointed to serve at the same time shall be of the same political party. Each member shall be appointed from the public at large and not from among officers or employees of the United States. Membership on the Board shall be the sole employment of each member.

"(c) COMPENSATION.—Members of the Board shall be compensated at the rate provided for GS–18 under section 5332 of title 5 of the United States Code.

"(d) CHAIRMAN.—The Chairman of the Board shall be elected by the Board every two years.

"(c) STAFF.—The Board shall appoint and fix the compensation of such personnel as are necessary to the carrying out of its duties.

"FUNCTIONS OF THE BOARD

"SEC. 8. The Board shall—

"(1) publish an annual Data Base Directory of the United States containing the name and characteristics of each personal information system maintained by a Federal agency;

"(2) make rules to assure compliance with this Act;

"(3) perform or cause to be performed such research activities as may become necessary to implement this Act, and to assist Federal agencies in complying with this Act;

"(4) be granted admission at reasonable hours to any federally controlled premises where any information system is kept or where computers or equipment or recordings for automatic data processing are kept, and may by subpena compel the production of documents relating to such information system or such processing as is necessary to carry out its duties, but no personal information shall be compelled to be produced without the prior consent of the data subject to which it pertains. Enforcement of any subpena issued under this section

shall be had in the appropriate United States district court;

"(5) upon the determination of a violation of a provision of this Act or regulation promulgated under the Act, the Board may, after opportunity for a hearing, order the Federal agency violating such provision to cease and desist such violation. The Board may enforce any order issued under this paragraph in a civil action in the appropriate United States district court;

"(6) conduct open, public hearings on all petitions for exceptions or exemptions from provisions, application, or jurisdiction of this Act. The Board shall have no authority to make such exceptions or exemptions but shall submit appropriate reports and recommendations to Congress; and

"(7) issue an annual report of its activities to the Congress and the President.

"TRADE SECRETS

"SEC. 9. In connection with any dispute over the application of any provision of this Act, no Federal agency shall reveal any personal information or any professional, proprietary, or business secrets; except as is required under this Act. All disclosures so required shall be regarded as confidential by those to whom they are made.

"CRIMINAL PENALTY

"SEC. 10. Any responsible officer of a Federal agency who willfully—

"(1) keeps an information system without having notified the Federal Privacy Board; or

"(2) issues personal information in violation of this Act;

shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

"CIVIL REMEDIES

"SEC. 11. (a) INJUNCTIONS FOR COMPLIANCE.—The Attorney General of the United States, on the advice of the Federal Privacy Board, or any aggrieved person, may bring an action in the appropriate United States district court against any person who has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this Act or rules of the Federal Privacy Board, to enjoin such acts or practices.

"(b) CIVIL LIABILITY FOR UNFAIR PERSONAL INFORMATION PRACTICE.—Any person who violates the provisions of the Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

"(1) any actual damages sustained by an individual;

"(2) punitive damages where appropriate;

"(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

The United States consents to be sued under this section without limitation on the amount in controversy.

"EFFECTIVE DATE

"SEC. 12. This Act shall take effect one year after the date of its enactment.".

PART 3—LEGISLATIVE DEBATE

Senate Action [1]

[From the Congressional Record—Senate, Sept. 19, 1974]

FEDERAL PRIVACY BOARD ACT—AMENDMENT

AMENDMENT NO. 1914

(Ordered to be printed and referred to the Committee on Government Operations.)

HALTING USE OF THE SOCIAL SECURITY NUMBER AS A UNIVERSAL POPULATION IDENTIFIER

Mr. GOLDWATER. Mr. President, I am introducing today for myself and the senior Senator from Illinois (Mr. Percy) an amendment to halt the spread of the social security number as a universal population identifier. I am delighted that the Senator from Illinois, who is the ranking Republican member of the Senate Committee on Government Operations, is joining with me today as a coauthor of this amendment to S. 3418, a privacy bill which was ordered favorably reported by that committee on August 20.

Mr. President, the amendment which we are offering today is similar to S. 2537, a bill which I introduced last year to provide that no individual may be compelled to disclose his social security number for any purpose not specifically required by law. An identical bill, H.R. 9968, had been introduced in the House of Representatives last year by my son, Congressman Goldwater, Jr., of California.

Mr. President, when parents cannot open bank accounts for their children without obtaining social security numbers for them; when all schoolchildren in certain ninth grade classes are compelled to apply for social security numbers; when a World War I veteran is asked to furnish his social securial number in order to enter a Veterans' Administration hospital; and when the account number is used and required for numerous other purposes totally unrelated with the social security program; then it is time for society to stop this drift toward reducing each person to a number.

There already have been issued a total of over 160 million social security numbers to living Americans. There is no statute or regulation which prohibits or limits use of the account number.

To the contrary, a directive President Roosevelt issued 32 years ago, is still in effect requiring that any Federal agency which establishes a new system of personal identification must use the social security number.

[1] For Senator Ervin's introductory remarks on S. 3418, see p. 3. Text of S. 3418 may be found on p. 9.

Numerous Americans deplore this development. They resent being constantly asked or required to disclose their social security number in order to obtain benefits to which they are legally entitled. They sense that they are losing their identity as a unique human being and are reduced to a digit in some bureaucratic file.

Scholars who have studied the situation have fears which run far deeper. These specialists consider use of the social security number as a population number will make us all become marked individuals.

What is meant is that once the social security number is set as a universal identifier, each person would leave a trail of personal data behind him for all of his life which could be immediately reassembled to confront him. Once we can be identified to the administrator in government or in business by an exclusive number, we can be pinpointed wherever we are, we can be more easily manipulated, we can be more easily conditioned and we can be more easily coerced.

Mr. President, the use of the social security number as a method of national population numbering is inseparable from the rapid advances in the capabilities of computerized personal data equipment. The state of the art in computer data storage is now so advanced that the National Academy of Sciences actually reported in 1972 that—

> It is technologically possible today, especially with recent advances in mass storage memories, to build a computerized, on-line file containing the compacted equivalent of 20 pages of typed information about the personal history and selected activities of every man, woman, and child in the United States, arranging the system so that any single record could be retrieved in about 30 seconds.

Where will it end? Will we allow every individual in the United States to be assigned a unique identification number for use in all his governmental and business activities? Will we permit computerized personal data systems to interlink nationwide so that all the details of our personal lives can be assembled instantly for use by a single person or institution?

The time to think about the future is now. We must build into the law safeguards for personal privacy while a national numbering system is still a concept and not an accomplished fact.

Accordingly, I am introducing today with Senator Percy an amendment to the Federal privacy legislation that will impose a moratorium on the use of social security numbers for purposes unrelated to the original social security program. Our amendment will make it unlawful for any governmental body at the Federal, State, or local level to deny to any person a right, benefit, or privilege because the individual does not want to disclose his social security account number. The amendment also provides that it shall be unlawful for anyone to discriminate against another person in any business or commercial dealings because the person chooses not to disclose his social security number.

Recognizing that what we are proposing will cause a significant change in the identification methods of a great many agencies and institutions, we provide for the phasing in of these prohibitions beginning on January 1, 1975. Any information system started after that date will be subject to the restraints of our amendment and any information system in existence before then is exempted from the amendment.

In addition to the prohibitions on the spread of the social security number in the future, the amendment includes a requirement that all

agencies and persons who request of a person the disclosure of his social security number must inform the person whether disclosure is mandatory or voluntary, state the specific authority for compelling disclosure, tell what uses will be made of it, and notify what rules of confidentiality will protect these uses.

Mr. President, medical and sociological evidence proves that the need for privacy is a basic, natural one, essential both to individual physical and mental health of each human being and to the creativity of society as a whole. It is for us to determine today just how much privacy shall remain for the individual in the future, and I hope the Senate will shortly have the opportunity to act favorably upon the amendment which we have offered to protect against a national numbering system.

Mr. President, I ask unanimous consent that a copy of the amendment by myself and Senator Percy, as coauthors, be printed in the Record.

There being no objection, the amendment was ordered to be printed in the Record, as follows:

AMENDMENT No. 1914

MORATORIUM ON USE OF SOCIAL SECURITY NUMBERS

SEC. 307. (a) It shall be unlawful for—

(1) any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number, or

(2) any person to discriminate against any individual in the course of any business or commercial transaction or activity because of such individual's refusal to disclose his social security account number.

(b) The provisions of subsection (a) shall not apply with respect to—

(1) any disclosure which is required by Federal law, or

(2) any information system in existence and operating before January 1, 1975.

(c) Any Federal, State, or local government agency which requests an individual to disclose his social security account number, and any person who requests, in the course of any business or commercial transaction or activity, an individual to disclose his social security account number, shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

Mr. PERCY. Mr. President, the issue of the social security number, SSN, as a universal identifier, which increasingly is required to be supplied by an individual in his transactions with both the Government and with private businesses, and which may soon make it possible for anyone to link and gain access to a wide variety of different databanks, is a matter of deep concern to me and to other Members of the Senate and the House. I am pleased to join Senator Goldwater, who over an extended period of time has taken a very active, constructive concern in this issue, as cosponsor of an amendment to S. 3418 which addresses this concern and commend Senator Goldwater, my distinguished colleague, on his leadership in this important matter to every citizen.

S. 3418 is the privacy legislation that I have cosponsored with Senators Ervin, Muskie, and Ribicoff. The bill, which was unanimously reported by the Committee on Government Operations on August 20, establishes certain rights of privacy that apply to an individual's personal information. The bill also establishes a study commission, the

Federal Privacy Commission, whose primary functions will be to oversee and assist Federal agencies in the implementation of this Act and to conduct a study of a wide variety of privacy issues that, for lack of adequate information and understanding, are not covered in S. 3418.

A very important subject that the Commission will study is the use of the SSN as a universal identifier. This study will respond to concerns of a wide variety of individuals who have expressed their resentment in letters to Members of Congress in recent years about having to furnish their SSN for purposes completely unrelated to social security.

The purpose of the amendment we are proposing is to halt the expansion of the use of the SSN. Its primary importance is to hold the problem to a fixed dimension until the Privacy Commission completes a study and decides upon appropriate legislative recommendations to Congress. It follows the key recommendations of the widely cited Report of the Secretary of HEW's Committee on Automated Personal Data Systems, published in 1973 under the title "Records, Computers, and the Rights of Citizens." On page 126 of the report, the HEW Committee gives specific recommendations on the SSN concerning the right of an individual to refuse to disclose the social security number:

SPECIFIC RECOMMENDATIONS ON THE SOCIAL SECURITY NUMBER RIGHT OF AN INDIVIDUAL TO DISCLOSE THE SOCIAL SECURITY NUMBER

Increasing demands are being placed on individuals to furnish an SSN in circumstances when use of the SSN is not required by the Federal Government for Federal program purposes. For example, the SSN is demanded of individuals by State motor vehicle departments, by public utility companies, landlords, credit grantors, schools, colleges, and innumerable other organizations.

Existing Federal law and Social Security regulations are silent on such uses of the SSN. They provide no clear basis for keeping State and local government agencies and private organizations from demanding and using the number. As a practical matter, disclosure of one's SSN has been made a condition for obtaining many benefits and services, and legal challenges to this condition under State law have been almost uniformly unsuccessful.

If the SSN is to be stopped from becoming a "de facto" universal identifier, the individual must have the option not to disclose his number unless required to do so by the Federal government for legitimate Federal program purposes, and there must be legal authority for his refusal. Since existing law offers no such clear authority, we recommend specific, preemptive, Federal legislation providing:

(1) That an individual has the right to refuse to disclose his SSN to any person or organization that does not have specific authority provided by Federal statute to request it;

(2) That an individual has the right to redress if his lawful refusal to disclose his SSN results in the denial of a benefit, or the threat of denial of a benefit; and that, should an individual under the threat of loss of benefits supply his SSN under protest to an unauthorized requestor, he shall not be considered to have forfeited his right to redress;

(3) That any oral or written request made to an individual for his SSN must be accompanied by a clear statement indicating whether or not compliance with the request is required by Federal statute, and, if so, citing the specific legal requirement.

In response to these recommendations, our amendment to S. 3418 prohibits Government agencies from conditioning any right, benefit, or privilege provided by law upon an individual's decision not to disclose his SSN. It would also prohibit discrimination against any indi-

vidual who, in the course of any business or commercial transaction or activity, chooses not to furnish his number. Finally, the amendment requires that whenever a Federal agency or private organization requests an individual to supply his SSN, it must inform him whether disclosure is mandatory or voluntary, by what statutory authority the number is requested, what uses will be made of it, and what rules of confidentiality will govern it.

I would like to point out that our amendment fills a void created when an earlier provision was dropped from S. 3418. It would have prohibited Government and private organizations that currently rely on the SSN from compelling an individual to furnish his number except when specifically required by law. The members of the Government Operations Committee voted to delete this provision after several important objections were identified. These objections centered around the disruption of established procedures and uncertain but large cost involved in changing recordkeeping procedures nationwide. The earlier provision would have meant redesigning forms and reprograming computers to an unknown extent. It would have had the undesirable effect of requiring the Army to change their identification system for military personnel.

Our amendment overcomes the flaws in the earlier provision. It does not interfere with existing uses of the number. It specifically exempts any disclosure which is required by Federal law and it exempts any use of the SSN by any information system that is in existence and operating prior to January 1, 1975. Thus it will not disrupt established procedures and it will not create unwarranted cost burdens. Instead, it serves the important function of blocking further expansion of the use of the number as a universal identifier until needed policy recommendations can be developed by the Federal Privacy Commission. And finally, it brings needed congressional attention to an issue of long standing.

[From the Congressional Record—Senate, Nov. 21, 1974]

SENATE CONSIDERS S. 3418 AS REPORTED BY THE COMMITTEE ON GOVERNMENT OPERATIONS

The Senate continued with the consideration of the bill (S. 3418) to establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State and local governments, and other organizations regarding such information, and for other purposes.

Mr. HRUSKA. Mr. President, I ask unanimous consent on behalf of the Senator from Arkansas (Mr. McClellan) and of myself for the privilege of the floor during consideration of S. 3418 and voting thereon of Mr. Paul C. Summitt, Dennis G. Thelan, J. C. Argetsinger, and Douglas Marvin.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. GOLDWATER. Mr. President, I ask unanimous consent that during the proceedings this afternoon on S. 3418 my legal assistant, Terry Emerson, be allowed the privilege of the floor.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from North Carolina.

Mr. ERVIN. Mr. President, I ask unanimous consent that Robert B. Smith, Jr., Al From, W. P. Goodwin, Jr., David Johnson, Bob Vastine, Mark Bravin, Marrilyn Harris, Wright Andrews, Jim Davidson, Gretchen MacNair, Mark Gitenstein, W. Thomas Foxwell, and Elizabeth Preast of the staff of the Committee on Government Operations be allowed the privilege of the floor at all times during the consideration of S. 3418, including all votes thereon.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. ERVIN. Mr. President, S. 3418 was originally introduced by myself with the cosponsorship of the distinguished Senator from Illinois (Mr. Percy), the distinguished Senator from Maine (Mr. Muskie), the distinguished Senator from Connecticut (Mr. Ribicoff), the distinguished Senator from Washington (Mr. Jackson), the distinguished Senator from Arizona (Mr. Goldwater), and the distinguished Senator from Tennessee (Mr. Baker).

Since that time the following Senators have been made cosponsors of the bill the distinguished Senator from Tennessee (Mr. Brock), the distinguished Senator from Michigan (Mr. Hart), the distinguished Senator from California (Mr. Cranston), the distinguished Senator from Massachusetts (Mr. Kennedy), the distinguished Senator from New York (Mr. Buckley), the distinguished Senator from Minnesota (Mr. Humphrey), and the distinguished Senator from Maryland (Mr. Mathias).

Mr. President, to facilitate the consideration of the bill, I ask unanimous consent that the committee amendment of the Committee on Government Operations in the nature of a substitute be agreed to and that the committee amendment as agreed to be considered original text for the purposes of further amendment.

The PRESIDING OFFICER. Is there objection? The Chair hears none. Without objection, it is so ordered.

The committee amendment in the nature of a substitute may be found on p. 97.

CONSIDERATION OF PERFECTING AMENDMENTS

Mr. ERVIN. Mr. President, after the committee had reported the bill, the committee staff worked out a number of amendments with the Office of Management and Budget and also other perfecting amendments which I send to the desk at this time and ask they be voted on en bloc.

The PRESIDING OFFICER. The clerk will report the amendments.

The legislative clerk read as follows:

On page 26, line 21 immediately after the period insert the following new sentence: "A subpena shall be issued only upon an affirmative vote of a majority of all members of the Commission.".

On page 31, line 1, strike out "travel, hotel, and entertainment res-" and insert in lieu thereof "cable television and other telecommunications media, travel, hotel, and entertainment res-".

On page 33, line 10, strike out all after "(1)" up to the semicolon on line 13, and insert in lieu thereof the following: "insure that personal information maintained in the system or file is accurate, complete, timely, and relevant to the purpose for which it is collected or maintained by the agency at the time any access is granted to the file, material is added to or taken from the file, or at any time it is used to make a determination affecting the subject of the file."

On page 34, line 22, strike out all that follows through the period on line 24, and insert in lieu thereof the following: "Such information is relevant and necessary to carry out a statutory purpose of the agency."

On page 37, line 15, strike out all through the semicolon on line 17 and insert in lieu thereof the following new subparagraph:

"(D) to know the sources of personal information (i) unless the confidentiality of any source is required by statute, then the right to know the nature of such source; or (ii) unless investigative material used to determine the suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, is compiled by a Federal agency in pursuit of an authorized investigative responsibility, and in the course of compiling such materials, information prejudicial to the subject of the investigation is revealed through a source who furnishes such information to the Government under the express provision that the identity of the source will be held in confidence, and where the disclosure of such information would identify and be prejudicial to the rights of the confidential source, then the right to know the nature of such information and to examine that information if it is found to be material or relevant to an administrative or judicial proceeding by a Federal judge or Federal administrative officer. Provided, that investigative material shall not be made available to promotion boards which are empowered to promote or advance individuals in Federal employment, except when the appointment would be from a noncritical to a critical security position."

On page 38, line 15, after "relevant" strike the comma and insert the following: "to a statutory purpose of the agency,".

On page 39, line 5, strike out all after "(F)" through line 8, and insert in lieu thereof the following: "Not later than sixty days after receipt of notice from an individual making a request concerning personal information, make a determination with respect to such request and notify the individual of the determination and of the individual's right to a hearing before an official of the agency which shall if requested by the individual, be conducted as follows:".

On page 39, line 9, immediately after "hearing" insert "shall be conducted in an expeditious manner to resolve the dispute promptly and".

On page 39, line 10, strike out "at which time" and insert the following:

"and, unless the individual requests a formal hearing, shall be conducted on an informal basis, except that".

On page 39, line 11, strike out "appeal" and insert in lieu thereof "appear".

On page 39, line 22, immediately after "reviewable" insert "de novo".

On page 39, between lines 23 and 24, insert the following: "An agency may, for good cause, extend the time for making a determination under this subparagraph. The individual affected by such an extension shall be given notice of the extension and the reason therefore."

On page 39, line 25, immediately after "agreement" insert "for", and.

On page 40, line 1, immediately before "of" insert ", or the operation by or on behalf of the agency".

On page 40, line 2, strike out "or" the second time it appears and insert in lieu thereof a comma.

On page 40, line 3, immediately after "alteration" insert ", or the operation by or on behalf of the agency".

On page 42, line 19, strike out "or the recipient".

On page 42, line 21, strike out "201(b)(4) and section".

On page 43, line 6, strike out "research or reporting" and insert in lieu thereof "reporting or research".

On page 43, line 10, strike out "safety, or identification" and insert in lieu thereof "or safety".

On page 43, line 13, strike out all through the period on line 17.

On page 43, line 18, strike out "(d)" and insert in lieu thereof "(c)"

On page 44, line 1, strike out "(e)" and insert in lieu thereof "(d)".

On page 44, line 12, strike out "(f)" and insert in lieu thereof "(e)".

On page 45, line 2, strike out the comma and insert in lieu thereof ";or".

On page 45, line 10, after the colon insert the following: "Provided that investigatory records shall be exempted only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) disclose the identity of a confidential source, and in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential in-

formation furnished only by the confidential source, (E) disclose confidential investigative techniques and procedures which are not otherwise generally known outside the agency, or (F) endangers the life or physical safety of law enforcement personnel."

On page 47, line 7, strike out "section 201(c)(3), (G), (I), and (J)" and insert in lieu thereof "sections 202(c)(3) (A), (B), (D), (E), (F), (G), (I), and (J)."

On page 47, between lines 23 and 24, insert the following new subsection:

"(d) The provisions of this Act shall not require the disclosure of testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service if the disclosure of such material would compromise the objectivity or fairness of the testing or examination process.".

On page 48, between lines 8 and 9, insert the following new section:

REGULATIONS

Sec. 207. Each Federal agency subject to the provisions of this Act shall, not later than six months after the date on which this Act becomes effective, promulgate regulations to implement the standards, safeguards, and access requirements of this title and such other regulations as may be necessary to implement the requirements of this Act.

On page 52, line 5, strike out "$10,000" and insert in lieu thereof "$2,000".

On page 52, line 6, strike out "five" and insert in lieu thereof "two".

On page 52, lines 22 and 23, strike out "has engaged, is engaged," and insert in lieu thereof "is engaged."

On page 53, line 1, strike out "Any" and all that follows through "liable" on line 3, and insert in lieu thereof the following: "The United States shall be liable for the actions or omissions of any officer or employee of the Government who violates the provisions of this Act, or any rule, regulation, or order issued thereunder in the same manner and to the same extent as a private individual under like circumstances".

On page 53, line 12, immediately after the period insert the following: "A civil action against the United States under subsection (c) of this section shall be the exclusive remedy for the wrongful action or omission of any officer or employee."

On page 47, between lines 23 and 24, insert the following:

(d) "The provisions of this Act, with the exception of Sections 201(a)(2), 201(b) (2), (3), (4), (5), (6), and (7), 201(c)(2), 201(c) (3) (A), (B), (D), and (F) and 202(a) (2) and (3) shall not apply to foreign intelligence information systems or to systems of personal information involving intelligence sources and methods designed for protection from unauthorized disclosure pursuant to 50 U.S.C.A. 403."

Mr. ERVIN. I might state to the Senate that none of these amendments makes any fundamental alteration in the bill. They merely clarify certain sections and make certain adjustments to satisfy some of the requests made by the Office of Management and Budget.

The amendments were agreed to en bloc.

Mr. ERVIN. Mr. President, I yield to the distinguished Senator from Connecticut with the understanding I do not thereby lose my right to the floor.

Mr. WEICKER. Mr. President, I ask unanimous consent that Mr. Bob Dotchin, Geoffrey Baker, and John Harvey of my staff be permitted the privilege of the floor during debate on this matter.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. WEICKER. I thank the distinguished Senator.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. ERVIN. Mr. President, I ask unanimous consent to insert in the Record at this point a memorandum which explains in detail the amendments to the bill that the Senate has just adopted.

There being no objection, the memorandum was ordered to be printed in the Record, as follows:

AMENDMENTS TO THE FEDERAL PRIVACY ACT

Attached are both technical and substantive Committee amendments to S. 3418 which have been drafted since this legislation was reported August 20 by the Committee on Government Operations. These amendments reflect an effort to improve S. 3418 and in part are based upon suggestions offered by OMB director, Roy Ash in a letter to Senator Ervin dated September 18, 1974.

TECHNICAL AND SUBSTANTIVE COMMITTEE AMENDMENTS

1. Section 105(a)(1) on page 26, line 21. It was intended in the bill as reported by the Government Operations Committee that no subpoena shall be issued by the Federal Privacy Protection Commission unless it was approved by a majority vote by all members of the Commission. While this point was covered indirectly in another section governing action by the Commission, it was felt necessary to clear up any ambiguity with an amendment which specifically states that requirement.

2. Section 201(b)(1) on page 33, line 10. As reported the bill requires that information maintained in agency systems or files be accurate, complete, timely, and relevant. Under these standards agencies would be required to search through all of their files and clean out any "dirty", inaccurate, or irrelevant material. In order to reduce the cost and administrative burden of such a requirement this amendment proposes to require the "cleaning up" of files at the time any access is granted to a file, material is added to or taken from a file, or at any time the file is used to make a determination affecting the subject of the file.

There may be an Administration amendment which would seek to require the cleaning up of files only at the time a determination is made affecting the subject of the file—a much weaker standard than proposed here.

3. Section 201(b)(7) on page 34, line 22. This section would prohibit agencies from establishing programs to collect or maintain information about how individuals exercise First Amendment rights. An exception is provided if an agency head specifically determines that the program is required for the administration of a statute which the agency is charged with administering. It seemed that a much tighter standard would be that used throughout the rest of the Act which would permit an exception only when "such information is relevant and necessary to carry out a statutory purpose of the agency."

4. Section 201(d)(1)(D) on page 37, line 15. This section requires that agencies disclose the sources of personal information unless the confidentiality of such sources is required by statute. In any other instance, however, agencies would be required under this Act to make available to the subject of the file any comments by third parties and identify those third parties in the record. While this requirement is not without merit the Civil Service Commission and other agencies express concern that confidentiality is necessary in soliciting candid comments during background investigations of persons to determine their suitability for employment for military service, to receive Federal contracts or to gain access to classified materials.

Should it be decided that protection is needed for certain third party comments, the attached amendments include a fairly restrictive draft amendment which would, in a case where disclosure of third party information would identify and be prejudicial to the rights of the confidential sources, permit the subject of the file to know only the nature of the information provided. However, if the information were to be found material or relevant to an administrative or judicial proceeding the judge or federal administrative officer could make it available to the subject of the file. A further proviso would require that such investigative material could be made available to promotion boards unless the appointment under consideration would be from a non-critical to a critical security position.

5. Section 201(d)(2)(F) on page 39, line 5. As the bill was reported, there was no time limit for the agency to respond to an initial request for information about his file. This amendment would set a limit for sixty days after receipt of notice from an individual requesting certain personal information for the

agency to make a determination with respect to such request and notify the individual whether the agency will provide the information and of his right to a hearing within the agency.

6. Section 201(d)(2)(F) on page 39, lines 9 and 10. These amendments require the agency to conduct hearings in an expeditious manner and permit the individual to request either a formal or informal hearing before the agency regarding requests to challenge certain information within a file.

7. Section 201(d)(2)(F)(ii) on page 39, line 22. This amendment provides for a Federal district court to review a petition to challenge personal data in a *de novo* proceeding. This is a technical amendment—albeit an important one—since it has always been assumed that appeals would be *de novo* in fact was so discussed in the Committee report. The actual wording was merely left out of the final draft.

8. Section 210(e) on page 40, line 1. It was felt that an amendment was needed to permit agencies to extend the safeguards of this Act to those private or State and local government contractors or grantees, in those limited situations covered by the bill where the contract or grant is for the specific purpose of creating or altering an information system, to the additional case where the contract or grant might specifically be for the operation by or on behalf of the agency. Apparently, Federal agencies do contract with private firms on a regular basis for the use of data processing and information facilities and this coverage is therefore necessary.

9. Section 202(b) on page 42, line 21. Strike out the words "201(b)(4) and Section". Under this general section, an agency would have to obtain the consent of an individual before it could transfer information out of its files about that individual to offices and employees of the agency in the ordinary course of their duties; to the Bureau of the Census to carry out a census or survey under the provisions of its act; where advance written notice has been obtained that the information provided will be used only as a statistical record; or whether it is a compelling circumstance affecting the health or safety of the subject of the file. As reported, the bill would also excuse the agency in the aforementioned circumstances from recording the persons or agencies to whom the information was distributed. On reflection, it was determined that this would not be a desirable feature and that all disclosures of information outside of the file should be recorded.

10. Section 203(b) on page 45, line 10. In the bill as recorded criminal investigative information would have had to be released after a period necessary to commence criminal prosecution. It was felt that the language of the Hart Amendment, adopted when the Congress passed the recent Amendments to the Freedom of Information Act, was a much more specific and carefully drawn provision for the ultimate release of criminal investigative records and that its language be substituted here since it had already received Justice Department approval.

11. Section 205 on page 47, between lines 23 and 24. The Civil Service Commission has made what appears to be a reasonable request that the Act not permit the disclosure of testing or examination material used solely to determine qualifications of an individual for appointment or promotion in the Federal service. In those instances where the disclosure of that material would compromise the testing of examination process—in other words, where the release of test scores would permit the transfer of that information outside an agency and require the frequent changing of Civil Service Commission exams.

12. Section 207. This would be a new section adding a specific requirement that Federal agencies subject to the provisions of this Act, within six months after the date on which the Act becomes effective—this would be one year and six months after the bill is signed into law—would be required to promulgate regulations to implement the standards, safeguards, and access requirements of the Act.

13. Section 303(c) on page 53, line 1 and on page 53, line 12. As it is now drafted, the civil liability under the Act runs against an individual employee of a Federal agency who might violate the provisions of the Act or a rule issued thereunder. It has been suggested that this is an unusual provision and that civil liabilities should run only against the agency itself. An individual suing under the Act, however, should be able to recover both actual and general damages and there should be included a provision for liquidated damages of say $1,000 into the assessed against the agency for a violation of the Act.

Mr. ERVIN. Mr. President, I think this bill as amended by the amendments just adopted, as well as by the committee substitute, constitutes landmark legislation.

Mr. President, S. 3418 represents the culmination of many months of work by the Committee on Government Operations to fashion legislation that will guarantee the rights of all Americans with respect to the gathering, use, and disclosure of information about them by the Federal Government. I might also add inferentially that this bill also represents the culmination of many years of work by the Judiciary Subcommittee on Constitutional Rights.

A debt of gratitude is owed to two members of the committee in particular—Senator Percy of Illinois, the ranking minority member, and Senator Muskie of Maine, the chairman of the Subcommittee on Intergovernmental Relations.

Senator Percy supplied much of the initiative behind the introduction of the bill and much of the manpower behind its development in the committee.

Senator Muskie's contributions to the bill have been invaluable. He and his able staff on the Subcommittee on Intergovernmental Relations have been largely responsible for the reasonable and sensible approach that is embodied in the bill before us today.

Of course, praise must go to all members of the Committee on Government Operations. Without their many valuable contributions, we would have been unable to develop the sensible bill that the committee reported unanimously to the Senate.

Mr. President, S. 3418 establishes a Federal Privacy Commission and provides for safeguards and standards which Federal agencies must follow in the collection, maintenance, and dissemination of information about individual Americans.

The bill applies to the departments and agencies of the Federal executive branch.

In addition, a department or agency may apply its provisions to a personal data bank or a personal information system which is specifically created or substantially altered through a grant, contract, or agreement with that department or agency.

The reforms wrought by S. 3418 have been a long time coming. This is true despite the fact that the principles it implements, of fair, honest, and responsible behavior by Government toward its citizens, are those recognized values of Western jurisprudence and democratic constitutional government. More important, they are the principles upon which our own Constitution rests. Their restatement as legislative guarantees are vital today.

Somehow, the varied and wide-ranging functions which have been thrust very rapidly upon the Federal management machinery of an earlier time, have left great loopholes for the gathering, use and disclosure of information about Americans in ways and for reasons that should give us serious pause. The advent of computer technology and new ways of information storage and sharing which have made it possible for government to provide new services and to carry out new programs, have also encouraged the extension of some practices of doubtful wisdom or constitutionality. These practices have been sanctioned or tolerated by administrations regardless of the party in

power. For this reason the concern over the resulting threats to freedom has brought complaints to Congress from Americans in all walks of life.

These complaints have been examined by congressional committees, special Government studies, commissions, boards, and groups. They have been examined by private organizations and professional associations. Throughout our land, the subject of privacy has been debated as it applies for all citizens and as it applies to the needs of special groups.

Mr. President, it is my opinion that there is very little left to debate. I believe S. 3418 contains the minimum recommendations made for protecting privacy and for establishing constitutional rules for Government's use of computer technology for personal data systems.

This bill provides an information bill of rights for the citizen and a code of fair information practice for the departments and agencies of the executive branch. There have been many bills introduced to protect the privacy of certain groups of citizens. S. 3418 is legislation aimed at protecting the privacy of all Americans, whenever the Federal Government collects, keeps, or uses personal information from or about them.

Although many witnesses have said that the disclosures of Watergate highlighted the need for this bill, the committee report makes clear that the bill is based on long-standing complaints of governmental threats to privacy which will haunt Americans in the years ahead unless this legislation is enacted.

According to the report of the Government Operations Committee, the purpose of the bill is to:

> Promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use and disclosure of personal information about individuals.
>
> It is to promote accountability, responsibility, legislative oversight, and open government with respect to use of computer technology in the personal information systems and data banks of the Federal government and with respect to all of its other manual or mechanical files.
>
> It is designed to prevent the kind of illegal, unwise, over-broad, investigation and record surveillance of law-abiding citizens which has resulted in recent years from actions of some over-zealous investigators, from the curiosity of some government administrators, and from the wrongful disclosure and use of personal files held by Federal agencies.
>
> It is to prevent the secret gathering of information or the creation of secret information systems or data banks on Americans by employees of the departments and agencies of the Executive branch.
>
> It is designed to set in motion a long-overdue evaluation of the needs of the Federal government to acquire and retain personal information on Americans, by requiring stricter review within agencies or criteria for collection and retention of such information.
>
> It is also to promote observance of valued principles of fairness and individual privacy by those who develop, operate and administer other major institutional and organizational data banks of government and society.

The bill accomplishes these purposes in five major ways:

First, title I of the bill establishes an independent Privacy Protection Commission with subpena power and authority to receive and investigate charges of violations of the act and report them to the proper officials; to develop model guidelines and assist agencies in implementing the act; and to alert the President and Congress to proposed

Federal information programs and data banks which deviate from the standards and requirements of the act.

The Commission is also directed to make a study of the major data banks and computerized information systems of other governmental agencies and of private organizations and to recommend any changes in the law governing their practices, including the application of all or part of this legislation in order to protect the privacy of the individual.

Second, it requires agencies to give detailed notice of the nature and uses of their personal data banks and information systems and their computer resources. It requires the new Privacy Commission to maintain and publish a directory for the public of Federal data banks and personal information systems, a citizen's guide to personal files; to examine executive branch proposals for new personal data banks and systems, and to report to Congress and the President if they adversely affect privacy and individual rights. It penalizes those who keep secret such a personal information system or data bank.

Third, the bill establishes certain minimum information-gathering standards for all agencies to protect the privacy and due process rights of the individual and to assure that surrender of personal information is made with informed consent or with some guarantees of the uses and confidentiality of the information. To this end, it charges agencies to do the following things:

To collect, solicit, and maintain only personal information that is relevant and necessary for a statutory purpose of the agency;

To prevent hearsay and inaccuracies by collecting information directly from the person involved as far as practicable;

To inform people requested or required to reveal information about themselves whether their disclosure is mandatory or voluntary, what uses the penalties are involved and what confidentiality guarantees surround the data once Government acquires it; and

To establish no program for collecting or maintaining information on how people exercise first amendment rights without a strict reviewing process based on a statutory duty.

Fourth, title II of the bill establishes certain minimum standards for handling and processing personal information maintained in the data banks and systems of the executive branch; for preserving the security of the computerized or manual system; and for safeguarding the confidentiality of the information. To this end, it requires every department and agency to insure, by whatever steps they deem necessary:

That the information they keep, disclose or circulate about citizens is as accurate, complete, timely and relevant to the agency's needs as possible.

That they refrain from disclosing it within an agency unless necessary for employee duties, or from making it available outside the agency without the consent of the individual and proper guarantees for confidentiality, unless pursuant to open records laws or unless it is for certain law enforcement or other purposes which are cited in the bill.

That they establish rules of conduct with regard to the ethical and legal obligations of all employees and others involved in handling per-

sonal data, and take action to instruct all employees of such duties and of the requirements of this act.

That they issue appropriate administrative orders, provide personnel sanctions, and establish appropriate technical and physical safeguards to insure the security of the information systems and the confidentiality of the data.

That they not sell or rent the names and addresses of people whose files they hold.

That a person may, upon request, have his or her name removed from a mailing list maintained by a private organization.

That agencies make an effort to notify a person before surrendering personal data in response to compulsory legal process.

That they take positive steps to assure that the technological features of their automated data systems reflect the needs of Government to prevent unauthorized access and dissemination.

That they report to the Commission and to Congress when they propose centralizing computer resources and facilities involving storage, processing, or use of personal information.

Fifth, to aid in the enforcement of these legislative restraints, the bill provides administrative and judicial machinery for oversight and for civil remedy of violations. To this end, the bill gives the individual the rights, with certain exceptions, to be told upon request whether or not there is Government information on him or her, to have access to it to determine its accuracy and relevance, and to challenge it with a hearing upon request, and with judicial review in the Federal court—section 201(d).

The provisions of title III establish judicial remedies for the enforcement of the act through the courts by individuals and organizations in civil actions challenging denial of access to personal information or through civil suits by the Attorney General or any aggrieved person to enjoin violations of the act.

Mr. President, Senate Report No. 93–1183 contains a section-by-section analysis of the provisions of the bill. I commend this analysis to critics of this proposal.

I believe the committee's careful explanation of the background and purpose of the text of the bill provides a satisfactory response to most questions about the effect of the bill.

In many instances, this language reflects testimony and advice from witnesses, expert consultants, and advisers, as well as consultation with agencies and groups concerned about the possible impact of the legislation.

EXECUTIVE BRANCH VIEWS

The bill has been revised to deal with some legitimate problems raised by some private organizations and by some departments and agencies of the executive branch.

Despite these extensive revisions, some in the Federal Government still see legal ghosts. From the administration's lengthy list of objections to S. 3418, it almost appears that nothing but deletion of the major provisions of the bill will satisfy some people in the executive branch.

Mr. Philip Buchen testified before the committee on behalf of the White House Domestic Council on Privacy. The burden of his testi-

mony was that the problems of privacy and confidentiality are so varied and complex that they are beyond the legislative capacities of Congress to address in a comprehensive bill imposing similar standards on all agencies.

I disagree with those who hold this view. I believe the need has been demonstrated for a rule of law concerning the technology, policies, and practices of Government which affect the freedoms of Americans.

The committee asked the Office of Management and Budget for a report on S. 3418. They replied with a draft of a bill which represented their approach to these "complex" matters, by doing little more than affording the individual the opportunity to challenge inaccurate information used to make a decision about the person.

Mr. President, the committee response to the administration views and to this counterproposal from the Office of Management and Budget is set forth in the committee report on page 16 as follows:

> The Committee is convinced that effective legislation must provide standards for and limitations on the information power of government. Providing a right of access and challenge to records, while important, is not sufficient legislative solution to threats to privacy. Contrary to the views of Administration spokesmen, it is not enough to tell agencies to gather and keep only data which is reliable by their rights for whatever they determine is their intended use, and then to pit the individual against government, armed only with a power to inspect his file, and a right to challenge it in court if he has the resources and the will to do so.
>
> To leave the situation there is to shirk the duty of Congress to protect freedom from the incursions by the arbitrary exercise of the power of government and to provide for the fair and responsible use of that power. For this reason, the Committee deems especially vital the restrictions in section 201 which deal with what data are collected and by what means. For this reason, the establishment of the Privacy Commission is essential as an aid to enforcement and oversight.

Mr. President, a month after this bill was unanimously approved by the Government Operations Committee, we received a second communication concerning S. 3418 from Mr. Roy Ash, Director of the President's Office of Management and Budget. He expressed concern about the wisdom of passing the bill in its present state.

His first objection was to the coverage of the bill to State and local government and the private sector. This coverage has now been deleted.

His second objection was that the creation of an independent agency to implement the act was unnecessary and counterproductive, and would fragment responsibility. He advised us to delete title I of the bill establishing the Privacy Commission, and "thus let the agencies police themselves."

It is, however, the judgment of the Committee that such a Commission is necessary to assist in implementing the bill, to police violations, and to assist both Congress and the executive branch in controlling the Federal Government's incursions of the privacy of Americans. Clearly, responsibility could not be more fragmented than has been demonstrated in recent years. The Commission's efforts would coordinate efforts to protect privacy and would develop the kind of systematic reporting and information to allow all branches of Government and all levels of government to perform the duties assigned them by the constitutions and laws of this country.

The White House also objected to section 201(a)(3) which requires the department or agency to tell the person requested or ordered to

disclose information, whether that disclosure is mandatory or voluntary, what penalties or consequences will result from nondisclosure, and what confidentiality rules will govern the response.

Administration spokesmen felt this would have "the adverse effect of encouraging coercive data-gathering practices by emphasizing the penalties of not answering a request."

In my view, this argument is on a par with old-fashioned horse-trading. I believe the committee has answered it at length on pages 48 and 49 of the committee report.

The administration also objected to section 201(b)(1) which established for the first time a standard for all departments and agencies in the quality of their management of personal records. It is a management principle which has been largely ignored in the rapid growth of the Federal Government's size and services. With the intense efforts by the General Services Administration and the Office of Management and Budget to create uniform standards and to extend automation of records in all agencies, there is an immediate need for such a legislative mandate so that administrators make such considerations an essential element of management for all records systems. It is no longer sufficient to wait until one individual file is produced for the purpose of making a decision on one individual. There is something more than efficiency at stake here. The ease of producing computer printouts with information about many people, the technological ease of producing "enemies lists" from great masses of stored information, should give serious pause to those who agree too quickly with the White House argument.

The administration has also objected to section 201(f)(1) requiring reporting of proposed data banks on people and proposed sharing and centralizing of computer facilities. They urge instead, "that agencies be held accountable by a system of public scrutiny, for assuring that privacy concerns are assessed before any personal record-keeping system is implemented." They claim that regulations to this effect are being developed by the Domestic Council Privacy Committee. It is clear that public scrutiny is not sufficient to protect our constitutional liberties in the face of the complex scientific and administrative problems which make it difficult for anyone other than an expert in this field to understand what is going on until it is almost too late.

President Ford himself, as Vice President, explained the dangers to freedom when agencies are left to their own pursuits where computers and data are involved. He has stated about the recent proposal for FEDNET:

> I am concerned that Federal protection of individual privacy is not yet developed to the degree necessary to prevent FEDNET from being used to probe into the lives of individuals. Before building a nuclear reactor, we design the safeguards for its use. We also require environmental impact statements specifying the anticipated effect to the reactor's operation on the environment. Prior to approving a vast computer network affecting personal lives, we need a comparable privacy impact statement. We must also consider the fallout hazards of FEDNET to traditional freedoms.

I think this is too vital an issue to be left to an ad hoc committee of the Domestic Council. It is a matter in which Congress has the duty and the right to establish the procedures for effective oversight and for accountability to the rights of the American people.

Mr. President, the background of this legislation, going back many years, is described in the committee report. It is also set forth in the two volumes of the published hearings conducted by the Government Operations ad hoc Subcommittee on Information Systems and the Judiciary Subcommittee on Constitutional Rights.

I might state that there have never been more complete hearings held on any legislative proposal than have been held by the subcommittees.

The support for this legislation is found in these hearings and in the investigations conducted over many years by the Subcommittee on Constitutional Rights, whose members have diligently and patiently pursued governmental invasions of privacy wherever they arose.

Mr. President, pages 3 through 17 of the committee's report describe the background of this legislation and sets forth some examples of unwarranted invasions of privacy.

I wish to direct attention to a clerical error in the report on page 13 in the section entitled, "First Amendment Programs: The Army."

The first sentence should read:

Section 201(b)(7) prohibits departments and agencies from undertaking programs for gathering information on how people exercise their First Amendment rights unless certain standards are observed.

Mr. President, S. 3418 as reported by the Committee on Government Operations represents a very sensible approach to the protection of the individual right of privacy with respect to information collected, used, and maintained by the Federal Government. It represents an important first step in the protection of our individual right to be left alone, and I strongly urge all Senators to vote for this important legislation.

Mr. President, I would like to express my appreciation for the outstanding work of the staff of the Committee on Government Operations in perfecting this bill. Robert Bland Smith, Jr., the chief counsel and staff director, and J. Robert Vastine, the minority counsel, exerted formidable leadership over the efforts of the staff. They were extremely instrumental in securing consideration of this bill by the committee.

They were assisted most admirably by Jim Davidson, counsel to the Subcommittee on Intergovernmental Relations; W. P. Goodwin, Jr., counsel to the committee; and W. Thomas Foxwell, the committee's staff editor who had the burden of producing the voluminous printed record of the bill compiled by the committee.

Marcia J. MacNaughton, the committee's chief consultant on this bill—who, incidentally, spent several years on the staff of the Subcommittee on Constitutional Rights—and Mark Bravin, special consultant to the minority, made monumental contributions to the bill. Al From, aide to Senator Muskie, was also of great assistance to the committee.

SENATOR PERCY'S REMARKS ON S. 3418

Mr. PERCY. Mr. President, in 1890, Louis Brandeis wrote an historic essay for the Harvard Law Review. In that essay he noted that an advancing communications technology imperiled the individual's right of privacy. Brandeis pointed to the development of the telephone and the snapshot camera as mechanical devices that would seriously and irrevocably alter a person's fundamental right to be let alone. He

warned legislators and legal scholars of his time that a "next step" was needed to protect that right. That "next step" is long overdue.

Today, 84 years later, now that we have very sophisticated electronic bugging devices, we have computers, the type of devices Brandeis probably never even conceived of. I hope that we are prepared to take that next step by passing legislation to safeguard privacy.

Communications technology has now achieved a speed and facility that far outstrips anything Brandeis may have dreamed possible. It is increasingly apparent that in the long series of technological breakthroughs that have made the gathering, use and trading of personal data both efficient and economical, privacy safeguards have simply not kept pace. This has resulted in a tremendously increased potential for damaging misuse of personal information, and burgeoning abuses of our privacy.

Today, almost every fact about us is on file somewhere in this country. Federal census surveys record our household, family, and personal lives. The Internal Revenue Service gathers our income tax data. Motor Vehicle Registries keep track of our driving records and automobile ownership. Credit card files reveal how we spend our money and credit reporting companies monitor how we pay our bills. Hospital and physician files register intimate facts about our physical and mental well-being. Police agencies account for our dealings with the law and law enforcement agencies. Schools retain teachers' comments and records of our academic achievement and social adjustment. The list may be virtually endless because new systems of files are constantly being created.

In and of itself, any one of these personal files is not particularly ominous. Most people readily accept the fact that data gathering systems are necessary to our institutions if they are to keep pace with the complex needs of a modern society. Without records there would be chaos. The real problem comes, however, when these information systems are linked with one another and are used to exchange information without the knowledge or consent of the individuals concerned. When personal data collected by one organization for a stated purpose is used and traded by another organization for a completely unrelated purpose, individual rights could be seriously threatened.

I hope that we never see the day when a bureaucrat in Washington or Chicago or Los Angeles can use his organization's computer facilities to assemble a complete dossier of all known information about an individual. But, I fear that is the trend. Many of our Federal agencies have become omniverous fact collectors—gathering, combining, using, and trading information about persons without regard for his or her rights of privacy. Simultaneously, numerous private institutions have also amassed huge files and information retrieval systems containing millions of files of unprotected information on millions of Americans. Our ability as individuals to control access to personal information about us has all but completely faded.

To illustrate our inability to control personal data, consider the term "data banks." This metaphor is really inappropriate. Unlike the usual banks where an individual generally has the sole right to determine the contents of his accounts, the contents of a data bank are seldom deposited exclusively by the individual and they seldom, if

ever, can be withdrawn by him. Instead, information is collected from multiple sources by numerous organizations and it is drawn upon by whoever purchases or otherwise acquires access to it.

Unlike our personal bank statement which is checked for inaccuracies at least monthly by us and as often as daily by the institutions who keep our accounts, our data bank accounts are seldom if ever checked for accuracy and completeness.

Thus the individual is not the depositor, not the beneficiary, and not the guardian of personal information stored in a data bank. He is given little or no opportunity to see the information kept on him, and only rarely can he challenge the accuracy of that information. And yet this same information is used by all manner of organizations to make important decisions that may personally affect him. This must be corrected.

Where personal rights, benefits, privileges and opportunities are determined by the contents of an individual's file, he should be given the rights necessary to assure these determinations are based upon accurate up-to-date and relevant information. He should be kept fully aware of the uses to which personal data he is asked to disclose will be used. And this includes knowing what organizations will have access to his file and knowing the purposes for which they will use his data.

We have the opportunity here today to make an important beginning. The bill we are about to debate directs Federal employees to treat personal files with respect. Federal agencies are given a mandate to hold open public hearings to establish rules to protect the confidentiality of personal information they maintain. These open proceedings are an essential means of obtaining the input of trained privacy experts and private citizens, to assure that agency rules are responsible and equitable. Once these rules are determined, all Federal employees involved in the design and operation of systems of records on individuals must be trained to understand and to obey these rules.

When substantial changes or entire new computer systems are proposed by an agency, careful attention must at least be paid to their potential impact on personal privacy. These proposals must be evaluated by the Administration, by Congress and by privacy experts before they are so far along that they cannot be stopped even if they pose a serious and unwarranted threat to our personal privacy. If a proposal does not comply with the privacy standards in this act or with the privacy regulations of the agency involved, it will be set aside for 60 days. This will afford Congress and responsible executive branch officials an opportunity to decide what additional safeguards are needed or whether the project should be halted completely. Our proposed oversight mechanism is designed to force adequate consideration by Federal agencies of the privacy impact of their proposals. President Ford has strongly endorsed this analysis of new systems. It is intended to give high visibility to the trend toward more centralized files and to permit us to make informed decisions about our information practices in this country.

S. 3418 will cause the Federal Government to exercise caution and a new balanced judgment when considering proposals to implement new computer data systems and new techniques for handling personal information. This is essential to the broader purposes of the bill, which

must be emphasized. First, the bill establishes legal rights that permit the individual to exercise considerable control over his personal data. These rights are given substance through a carefully drawn set of information management requirements for Federal agencies backed by court review and enforcement. These individual rights and their corresponding agency requirements have been carefully studied by an impressive number of organizations, both in and out of Government. The chief recommendations of the 1973 HEW privacy report, perhaps the most widely cited of all privacy studies, have been embodied in S. 3418.

To understand how our bill provides these rights to every individual, I think we might consider a hypothetical example. Let us suppose, once S. 3418 is put into effect, that an individual hears about an information system called the National Driver Register. He could consult the U.S. Directory of Information Systems, which must be compiled by the Privacy Commission, and learn that this particular data system is maintained by the Department of Transportation. Reading the directory he would learn that this particular information system holds approximately 3,300,000 files on persons whose licenses have been denied, suspended, or revoked in any State. He could see that the main office of the system is located here in Washington and he would find the name, address, and telephone number of the Department of Transportation official directly responsible for the maintenance and activity of the system. He would also find other pertinent facts about these files including why they are kept, what they are used for, and who has access to them.

Let us now suppose that this individual wants to know whether his name is in the National Driver Register or in other files kept by the Department of Transportation. Following procedures explained in the information systems directory, he could write to the Secretary of Transportation or the appropriate official in that Department and ask what files exist on him. Their reply must include a complete list of all files about him. Then, if he wishes, he may request to see his file. He may be required to pay for the production of copies if he wants them, but the fee can be no greater than the actual cost of reproduction.

Suppose that the DOT file indicates a conviction for a drunken driving offense for which he was actually acquitted. In this case, the individual can ask the Department of Transportation to investigate the facts and make necessary corrections. If he gets no satisfaction from the Department within a reasonable period of time, he can demand an informal or formal hearing before the Agency. If even the hearing fails to resolve the dispute to his satisfaction, the individual may appeal his case to a district court of the United States. If the court decides in his favor, it may direct the Department to take appropriate corrective action and it may award damages to him, including reasonable attorney's fees.

Mr. President, these are the steps that our bill entitles a person to take to correct inaccurate or incomplete data kept about him by a Federal agency. This illustration demonstrates that the bill requires the Federal Government to be responsive to the rights of privacy and confidentiality. We cannot and do not allow an individual to be caught up in an endless struggle with the Federal bureaucracy to enforce

these rights. This is the first and most important contribution of S. 3418.

Another major purpose of S. 3418 is to establish a nonregulatory Commission. The Commission will perform two crucial roles, both as an adviser to Federal agencies who must implement this legislation, and as an adviser to Congress, recommending legislative solutions to the chief privacy problems of the private sector.

I believe that the Commission is a necessary part of this legislation, even though there has been strong controversy about its advisability. Our Federal agencies have expanded their information-gathering and surveillance activities to such an extent that they pose serious threats to our basic privacy rights. Until the agencies develop and adopt adequate rules and procedures, effective oversight can and must be performed by experts who understand the technology and yet who are sensitive to the basic question of how to safeguard privacy. This is a central reason for establishing the Commission. Equally important, I believe, is the need to develop effective solutions to privacy problems outside the realm of the Federal Government. This effort requires a concentration of talent and attention in a single unit. It also requires a clear mandate and adequate power to seek access to files, plans, and computer facilities. We have granted the Commission a limited authority to conduct studies and make recommendations to Congress and to the President. If this authority is exercised fully and properly, major questions of policy will be resolved by the Commission years before Congress could act through the committee hearing process.

An example of this need for the Commission to make informed policy decisions involves what I believe to be one of the most important symbols of the trend toward centralized records. I am speaking of the growing abuse of the social security number, for purposes completely unrelated to the social security system. The senior Senator from Arizona Mr. Goldwater, and I have introduced an amendment to S. 3418 to curb the expanding use of the social security number as a universal identifier, a single number that identifies each of us uniquely for all purposes. We are joined by the distinguished senior Senator from Washington, Mr. Magnuson. Our amendment will make it unlawful for any governmental body at the Federal, State, or local level to deny any person a right, benefit, or privilege simply because that individual does not want to disclose his social security number. The amendment also prohibits discrimination against a person in any business or commercial dealing because he chooses not to disclose his number. What we propose is to phase in restrictions so that any new use of the social security number initiated after January 1, 1975, will be subject to this amendment. Existing uses of the number will be allowed to continue pending the recommendations resulting from the formal study of the issue required of the Privacy Commission. But we must hold the problem to a constant size to permit this study to be complete and balanced.

Mr. President, the connection between the social security number and privacy is not at all obscure. Our number is used much as our name to identify us and to index our personal data. A striking example is contained in a report issued last year by the Federal Trade Commission. This report contains a formal Commission interpretation on

the sale of lists of individual credit ratings in what are called credit guides. These published credit guides, according to the FTC, demonstrate a lack of "respect for the consumer's right to privacy" and therefore constitute a violation of the Fair Credit Reporting Act.

The FTC opinion goes on to say that although publication of an individual's name together with his credit rating is an unacceptable invasion of privacy, it is perfectly permissible to publish the credit information together with individual social security numbers. I cannot understand how it is less of an invasion of privacy to use the social security number in this situation, especially when the number is so widely accessible.

Other examples exist in which an individual is actually deprived of the right to vote in a State or Federal election or to register for a driver's license if he refuses to disclose his social security number. There is the case of a telephone company in the Rocky Mountain area that has charged its customers a higher phone rate for failure to supply that number. Many of these coercive efforts to force an individual to supply this personal information have no basis in law. They certainly fly in the face of recommendations of the Social Security Administration and HEW and they defy my understanding of what is reasonable. Senator Goldwater and I have thus included a provision in our amendment that requires any government or private organization that requests an individual to disclose his social security number to inform that individual whether that disclosure is mandatory, or voluntary, by what statutory or other authority the number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

This provision is identical to a parallel provision in S. 3418. It is designed to promote openness by removing the element of intimidation from requests for personal data. It is intended to give back to each of us the freedom to choose the recipients and the circumstances in which our personal information is disclosed.

Mr. President, this bill is directly responsive to the publicly stated priorities of President Ford. Last March, the President promised delegates to the National Governors' Conference that action was soon to come. In June, he called for congressional action this year to pass a privacy bill. And on August 12 before a joint session of Congress, President Ford said:

> There will be hot pursuit of tough laws to prevent illegal invasions of privacy in both government and private activities.

Mr. President, the bill we have before us today is tough, yet reasonable. It is the product of years of research, both in and out of Government, and it is the product of several thousand man-hours of drafting effort by our staff, by the administration, and by a wide variety of private organizations. This bill is certainly not the final word on privacy. There will be additional laws needed to solve particular problems in such areas as medical files, records of scientific and statistical research, and credit files. But this bill is a historic beginning, a beginning which we owe in very great part to the distinguished Senator from North Carolina, Senator Ervin, who has devoted so much of a remarkable career to protecting personal freedoms.

In closing I would particularly like to commend the initiative of Robert Smith, chief counsel of the committee, and Robert Vastine, chief counsel to the minority, in expediting consideration of this bill. It was introduced as late as May 1 this year, and hearings were held on June 18. We have moved with deliberate speed to produce a carefully drafted bill. A great deal of the credit for this solid workmanship goes to Mark Bravin, of the minority staff, and James Davidson, of the majority staff, who made an especially important contribution to this effort. Marcia McNaughton and Marilyn Harris, both of the majority staff, each played an important role in preparation of this bill for our consideration today.

I might say also it is one other capstone that Senator Ervin places on a very distinguished career of service to the American people.

Mr. ERVIN. I commend the Senator from Illinois on the fine work that he did in this field. No Senator has been more interested in this subject or has devoted more hard work and study for this in the Senate bill and it merits the thanks of the American people for his services in respect to this.

Mr. President, as chairman of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, as well as the chairman of the Committee on Government Operations, I have studied this problem of privacy for many years, have conducted many hearings on the subject, have had the benefit of wise counsel of many experts in this field, and have read in large part the voluminous literature which has grown up around the question of privacy.

I think that this bill, in its present form, is about as fine a piece of legislation as can be drawn on this subject until we have the Privacy Board's experience to assist us in further refining the law.

I yield to the distinguished Senator from Nebraska.

SENATOR CURTIS' QUESTIONS REGARDING BUREAU OF THE CENSUS

Mr. CURTIS. I thank the distinguished Senator.

Mr. President, I wish to commend my distinguished friend for the thoroughness with which he has gone into this subject. It is a matter that merits the attention of the Congress. I wish to ask a question or two concerning the Bureau of the Census.

The junior Senator from Nebraska receives many compliments about the conduct of the Bureau of the Census. They sent out questionnaires consisting of many, many pages. Apparently, it is a selected list; it is not part of the 10-year enumeration. It asks for all sorts of information. Our citizens have two complaints against it. One is that it invades privacy. It asks all kinds of questions about their manner of living.

The second complaint is that it takes hours and hours to fill out the questionnaires, and there is a penalty imposed, a rather stiff penalty, if it is not filled out and returned.

Does this proposal repeal any of these laws that permit that?

Mr. ERVIN. Yes; I am glad that the Senator from Nebraska has called the attention of this Senator to this problem. I might state that, as he, I have received letters over the years.

In addition that that, I introduced a bill at one time to require the Bureau of the Census, when they send out a questionnaire, to advise the

person to whom it is sent whether it is mandatory for him to answer it or not. I was unable to get that bill passed.

There is a provision of law that if one fails to give the Bureau of the Census information which they are required by law to collect, he is guilty of a criminal offense and can be sent to jail for a relatively short period of time. As the Senator from Nebraska has indicated, the Bureau of the Census, on far too many occasions, sends out questionnaires about things that it is not required to investigate by law, and they fail to tell the people that they are not required to answer them.

I have had small businessmen in North Carolina inform me that they have been compelled on occasion to pay out substantial sums of money and devote many man-hours to answering these questionnaires, when, as a matter of fact, under the law, the Bureau of the Census has no right to compel them to answer. This bill deals with the subject by saying that no agency of the Government is allowed to solicit information from the American people unless the securing of such information is reasonable and necessary to enable an agency to perform some function that the law imposes upon it.

It further provides that when an agency, such as the Bureau of the Census, sends out a questionnaire, it must inform the people to whom the questionnaire is directed whether or not it is a mandatory or a voluntary questionnaire, and whether or not they are obliged by law to answer it. That will take care of the situation in large measure that the Senator is concerned about. I share his concern.

Mr. CURTIS. On every inquiry I have ever made, they come back and say that it is mandatory and threaten the people with punishment for not filling it out. It has nothing to do with the 10-year census. It is a total invasion of people's privacy.

Furthermore, it costs a lot of time and money to comply.

Mr. ERVIN. The Bureau of the Census, a few years ago, sent out a questionnaire to selected lawyers throughout the United States, just because some official of the American Bar Association suggested that it would be desirable for the American Bar Association to have the information. They wanted to know how much of a lawyer's practice was civil, how much was criminal, how much was counseling, and they wanted to know what he paid the secretaries, and things like that. They had no power to send out that questionnaire. This bill will put an end to that kind of questionnaire, because they have to tell the people whether they are required to answer it and under what law.

Mr. CURTIS. If the Senator will yield further, I shall submit another example. Fortunately, in this case, the Government bureau retreated and discontinued the practice.

The Committee on Finance has had the matter before it many times concerning the qualifications of individuals who assist citizens in making out their tax returns. The problem is very narrow. It consists of a not-too-large number of fly-by-night operators that advertise that they will save so much money on one's taxes. That is what the Committee on Finance had in mind when they talked about it.

It ended up in practice that the Internal Revenue Service moved into a small community in the State of Nebraska. This town has less than 1,500 people. It has a very distinguished lawyer there. They came into

his office and asked to see his files concerning every income tax he had made out. Then the Government proceeded to contact every one of his clients.

Nebraska is a very law-abiding State. People have respect for their Government. All they had to do to ruin this fine citizen was to state that the Government of the United States was investigating his practice, interviewing every one of his clients. He was an upright, law-abiding citizen of excellent reputation.

He secured a lawyer. I was advised of the matter. It was taken up with the Internal Revenue Service, and they discontinued it entirely. But we are not always that lucky. I have never gotten the Bureau of the Census to discontinue anything.

I wish there were something a little more specific here that really clips their wings and provides that when they send these scattered questionnaires out that go to just a few people, there absolutely could not be any penalty whatever.

Mr. ERVIN. There cannot. Under the law, there can be no penalty placed on any person for failing to respond to a questionnaire unless the questionnaire calls for information that the Bureau of the Census is required by law to collect.

Mr. CURTIS. They can always slip in one sentence of that. They come back to my citizens every time and say, "This is required by law and you are subject to a penalty."

Mr. ERVIN. If the Senator will pardon me, the Senator from Maine has an amendment and he has to leave at 4 o'clock. If the Senator from Nebraska will yield now, we shall let him introduce his amendment and then we shall return to the colloquy, because I am very much interested in this subject.

Mr. CURTIS. I thank the distinguished Senator.

AMENDMENT TO ENLARGE MANDATE BY SENATOR MUSKIE

Mr. MUSKIE. Mr. President, I thank the distinguished floor manager of the bill (Mr. Ervin).

I send my amendment to the desk and ask for its immediate consideration.

The PRESIDING OFFICER. The clerk will state the amendment.

The assistant legislative clerk proceeded to read the amendment.

Mr. MUSKIE. Mr. President, I ask unanimous consent that further reading of the amendment be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendment is as follows:

On page 25, line 16, strike out "and".

On page 25, line 21, strike out the period and insert in lieu thereof a semicolon and "and".

On page 25, between lines 21 and 22, insert the following new paragraph:

"(4) prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and discriminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation."

Mr. MUSKIE. Mr. President, as a cosponsor of S. 3418 and one who has followed the progress of Federal privacy legislation with great

interest for several years, I wish to express my support for this most important bill which is before the Senate today.

Many observers have characterized the 93d Congress as the "Privacy Congress." That appellation has been earned in large part by the effort and dedication of the foremost leader on this issue of individual rights—the distinguished Senator from North Carolina (Senator Ervin).

His concern, his persistence and his great knowledge built on years of judicial and legislative experience in this field, have brought us to the consideration of what could become a hallmark of his career—the Federal Privacy Act of 1974.

The privacy of our citizens has been a fundamental concern since the founding of our Republic. Two hundred years ago, William Pitt expressed this with regard to the rights of citizens in the colonies still under English rule:

> The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter—but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.

While the concern for the rights of American citizens to be secure from government invasion has run from the adoption of the Bill of Rights to present day times, it has not found widespread recognition in the courts outside of the area of criminal law. In applying the provisions of the fourth amendment to the Constitution to this issue, Mr. Justice Frankfurter observed in *Wolf* v. *Colorado* (338 U.S. 25, 27–28 1949):

> The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society . . . The knock at the door, whether by day or by night, as a prelude to a search, without authority of law but solely on the authority of the police, did not need the commentary of recent history to be condemned as inconsistent with the conception of human rights enshrined in the history and the basic constitutional documents of English-speaking peoples.

In a famous dissenting opinion in *Olmstead* v. *United States* (277 U.S. 438, 478 1938), Mr. Justice Brandeis characterized the "right to be let alone" by the Government as "the most comprehensive of rights and the right most valued by civilized men."

In his book, "The Assault on Privacy," Prof. Arthur Miller observed that while the fourth amendment was probably conceived to protect tangible objects, it has since been extended in *Katz* v. *United States* (389 U.S. 347, 353 1967) to restrict the Government's right to seize personal information.

While the courts have begun to recognize the capacity of Government to invade individual privacy by the gathering or misuse of information, it is the responsibility of the Congress to develop specific legislative guidelines in this area.

The Federal Privacy Act draws upon the constitutional and judicial recognition accorded to the right of privacy and translates it into a system of procedural and substantive safeguards against obtrusive Government information gathering practices.

Up until now we have allowed technological advances in Federal recordkeeping to outpace our efforts to control and safeguard the use

of the information we have collected. This act would balance those advances with specific safeguards and add a new dimension of rights to the citizen. In effect it would bring the law in line with a concept endorsed by then Secretary of Health, Education and Welfare, Elliot Richardson, that "Government is not the owner of information on individuals, but only the trustee."

Almost a year ago, the Subcommittee on Intergovernmental Relations, of which I am chairman, released a survey of individual attitudes toward their Government prepared by Louis Harris and Associates. That survey, revealed that the American people's loss of confidence in their Government had reached severe proportions. Forty-five percent of the public described themselves as alienated and disenchanted, feeling profoundly impotent to influence the actions of their leaders. The relationship between this feeling and the Government's invasion of individual privacy is underscored by a report by the Committee on Security and Privacy, of the Project Search task force authorized by the Department of Justice to examine the handling of criminal records. Calling for citizen right of access and challenge to certain law enforcement records, the search report stated:

> An important case of fear and distrust of computerized data systems has been the feelings of powerlessness they provoke in many citizens. The computer has come to symbolize the unresponsiveness and insensitivity of modern life. Whatever may be thought of these reactions, it is at least clear that genuine rights of access and challenge would do much to disarm this hostility.

S. 3418 is addressed to that very point. Under title II of this bill we have inserted the individual citizen into an active role regarding the collection, use and dissemination of his personal data by Federal agencies.

If an agency asks a citizen for information he would have the right to know if he is required to divulge it and to know what use the agency will make of it.

He would be entitled to know what information systems or files a Federal agency operates and whether those systems or files contain information about him.

He would be entitled to see what is in those files and if necessary to challenge the accuracy, the completeness, the timeliness and the relevancy to the needs of the agency of their contents.

He would be entitled to know who has seen information about him, and if the agency makes changes at his request, to inform past recipients of that data about those changes.

Finally, each citizen would be entitled to enforce this right of access and challenge in a Federal district court and to seek an award of damages for injuries resulting from the misuse of personal information.

These are fundamental rights to be included in any privacy legislation, and they should help begin to restore public faith in our Government's information practices.

The remarks which follow relate specifically to my amendments.

In considering this legislation it was understood that privacy considerations do not stop at the Federal Government. Our concern for the handling of information about individuals extends beyond Federal agencies to State and local government and to the private sector.

State government witnesses at the Government Operations Committee hearings in S. 3418 indicated the need to incorporate privacy safeguards in their information systems. Andre Atkinson, representing State and local government information system managers said:

> Effective solutions will come only from administrative and statutory regulations which can interact in concert at all levels of government—Federal, State and local.

While there have been extensive studies of information gathering systems operated by the Federal Government and the need for safeguards and regulation of those systems, the record still is incomplete about the information practices of State and local governments.

We have asked the Privacy Protection Commission established by this bill to examine those systems and recommend what legislation might be necessary in that area.

In the interim we can help those States and local governments which are attempting to deal with this issue now. I am offering an amendment to S. 3418 along with the distinguished Senator from Illinois, which would authorize the Commission to draft model privacy legislation for State and local governments and to make available to State and local officials the technical services of the Commission to aid in the preparation of privacy legislation to meet their needs.

I recognize that the establishment of the Privacy Commission has been the focus of some objection by the administration.

The need for an independent authority to examine Federal, State, and local and private information practices has received substantial support from the many witnesses who have testified in behalf of this bill.

It is not only essential to help the Congress and the executive branch to examine Federal practices, it can help bridge the gap between the standards we are setting for the Federal agencies and those we want to see adopted by other information systems outside the Government.

The assistance to State and local governments which would be provided by our amendment is but one example.

Mr. President, this is an important piece of legislation. I hope that this Congress will meet its responsibility and earn the label which it has already received as the Privacy Congress by passing S. 3418.

This, I think, Mr. President, is a very modest response to considerable pressures to expand this legislation to cover State and local governments as well as the private sector. It is for that reason that I submit the amendment to the Senate and urge its adoption.

I have discussed this proposal with Senator Ervin and with Senator Percy, who is a cosponsor of the amendment, and I believe they are in a position to accept it.

Mr. Percy. Mr. President, as a cosponsor of the amendment, I would simply like to indicate that, as a result of my work as a member of the Intergovernmental Commission, I believe certainly it is in the best interests of State and local governments to have the benefits now of all the magnificent work done by Senator Ervin through the years in preparing a piece of legislation at the Federal level. Certain of the States are moving in this direction now, but we ought to provide this as a service to all the States, and I am pleased to support the amendment as a cosponsor.

Mr. ERVIN. Mr. President, I think this is a very wise amendment. As I see it, the amendment would simply empower the Federal Privacy Board to assist the States in establishing privacy laws and privacy boards at the State level. It is not obligatory on anyone; it would merely enable the Federal Privacy Board, out of their experience and knowledge of the subject, to be of assistance to the States, and I would urge the Senate to adopt the amendment.

The PRESIDING OFFICER. The question is on agreeing to the amendment of the Senator from Maine.

The amendment was agreed to.

AMENDMENT NO. 1945

Mr. NELSON. Mr. President, I call up my amendment No. 1945.

The PRESIDING OFFICER. The amendment will be stated.

The assistant legislative clerk proceeded to read the amendment.

Mr. Nelson's amendment is as follows:

At the end of the bill, add the following new title:

"TITLE IV—JOINT COMMITTEE ON GOVERNMENT SURVEILLANCE AND INDIVIDUAL RIGHTS

"ESTABLISHMENT

"SEC. 401. (a) There is hereby established a Joint Committee on Government Surveillance and Individual Rights (hereinafter referred to as the "joint committee") which shall be composed of fourteen members appointed as follows:

"(1) seven Members of the Senate, four to be appointed by the majority leader of the Senate and three to be appointed by the minority leader of the Senate; and

"(2) seven Members of the House of Representatives, four to be appointed by the majority leader of the House of Representatives and three to be appointed by the minority leader of the House of Representatives.

"(b) The joint committee shall select a chairman and a vice chairman from among its members.

"(c) Vacancies in the membership of the joint committee shall not affect the power of the remaining members to execute the functions of the joint committee and shall be filled in the same manner as in the case of the original appointment.

"FUNCTIONS

"SEC. 402. (a) It shall be the function of the joint committee—

"(1) to make a continuing study of the extent and the method of investigation or surveillance of individuals by any department, agency, or independent establishment of the United States Government as such investigation or surveillance relates to the right of privacy, the authority for, and the need for such investigation or surveillance, and the standards and guidelines used to protect the right to privacy and other constitutional rights of individuals;

"(2) to make a continuing study of the intergovernmental relationship between the United States and the States insofar as that relationship involves the area of investigation or surveillance of individuals; and

"(3) as a guide to the several committees of the Congress dealing with legislation with respect to the activities of the United States Government involving the area of surveillance, to file reports at least annually and at such other times as the joint committee deems appropriate, with the Senate and the House of Representatives, containing its findings and recommendations with respect to the matters under study by the joint committee, and, from time to time, to make such other reports and recommendations to the Senate and the House of Representatives as it deems advisable; except that nothing in the foregoing provisions shall authorize the joint committee, or any subcommittee thereof, to

examine lawful investigative or surveillance activities related to the defense or national security of the United States conducted within the territorial boundaries of the United States citizens. For purposes of this subsection, lawful investigative or surveillance activities related to the defense or national security of the United States means investigative or surveillance activities carried on by duly authorized agencies to obtain information concerning unlawful activities directed against the Government of the United States which are substantially financed by, directed by, sponsored by, or otherwise involving the direct collaboration of foreign powers.

"(b) Nothing in this title shall give the joint committee, or any subcommittee thereof, jurisdiction to examine any activities of agencies and departments of the United States Government conducted outside the territorial boundaries of the United States.

"REPORTS BY AGENCIES

"SEC. 403. In carrying out its functions, the joint committee shall, at least once each year, receive the testimony, under oath, of a representative of every department and agency of the Federal Government which engages in investigations or surveillance of individuals, such testimony to relate to the full scope and nature of the respective agency's or department's investigations or surveillance of individuals, subject to the exceptions provided for in subsections 402(a)(3) and 402(b).

"POWERS

"SEC. 404. (a) The joint committee, or any subcommittee thereof, is authorized, in its discretion (1) to make expenditures, (2) to employ personnel, (3) to adopt rules respecting its organization and procedures, (4) to hold hearings, (5) to sit and act at any time or place, (6) to subpena witnesses and documents, (7) with the prior consent of the agency concerned, to use on a reimbursable basis the services of personnel, information, and facilities of any such agency, (8) to procure printing and binding, (9) to procure the temporary services (not in excess of one year) or intermittent services of individual consultants, or organizations thereof, and to provide assistance for the training of its professional staff, in the same manner and under the same conditions as a standing committee of the Senate may procure such services and provide such assistance under subsections (i) and (j), respectively, of section 202 of the Legislative Reorganization Act of 1946, and (10) to take depositions and other testimony. No rule shall be adopted by the joint committee under clause (3) providing that a finding, statement, recommendation, or report may be made by other than a majority of the members of the joint committee then holding office.

"(b)(1) Subpenas may be issued under the signature of the chairman of the committee or of any subcommittee, or by any member designated by such chairman, when authorized by a majority of the members of such committee, or subcommittee, and may be served by any person designated by such chairman or member.

"(2) Each subpena shall contain a statement of the committee resolution authorizing the particular investigation with respect to which the witness is summoned to testify or to produce papers, and shall contain a statement notifying the witness that if he desires a conference with a representative of the committee prior to the date of the hearing, he may call or write to counsel of the committee.

"(3) Witnesses shall be subpenaed at a reasonably sufficient time in advance of any hearing in order to give the witness an opportunity to prepare for the hearing and to employ counsel, should he so desire. The chairman of the joint committee or any member thereof may administer oaths to witnesses.

"(c) The expenses of the joint committee shall be paid from the contingent fund of the Senate from funds appropriated for the joint committee, upon vouchers signed by the chairman of the joint committee or by any members of the joint committee authorized by the chairman.

"(d) Members of the joint committee, and its personnel, experts, and consultants, while traveling on official business for the joint committee within or outside the United States, may receive either the per diem allowance authorized to be paid to Members of the Congress or its employees, or their actual and necessary expenses if an itemized statement of such expenses is attached to the voucher.

"(e)(1) The District Court of the United States for the District of Columbia shall have original jurisdiction, without regard to the sum or value of the matter in controversy, of any civil action heretofore or hereafter brought by the joint committee to enforce or secure a declaration concerning the validity of any subpena heretofore or hereafter issued by such joint committee, and the said District Court shall have jurisdiction to enter any such judgment or decree in any such civil action as may be necessary or appropriate to enforce obedience to any such subpena.

"(2) The joint committee shall have authority to prosecute in its own name or in the name of the United States in the District Court of the United States for the District of Columbia any civil action heretofore or hereafter brought by the joint committee to enforce or secure a declaration concerning the validity of any subpena heretofore or hereafter issued by such committee, and pray the said district court to enter such judgment or decree in said civil action as may be necessary or appropriate to enforce any such subpena.

"(3) The joint committee may be represented by such attorneys as it may designate in any action prosecuted by such committee under this title.".

On page 3, line 23, after "Act", insert "(other than title IV)".
On page 4, line 6, after "Act", insert "(other than title IV)".
On page 6, line 9, immediately after "of", insert "titles I, II, and III of".
On page 6, line 12, after "under", insert "titles I, II, and III of".
On page 7, line 1, immediately before "this", insert "titles I, II, and III of".
On page 7, line 2, immediately before "this", insert "title I, II, or III of".
On page 12, line 9, immediately before "this", insert "title I, II, or III of".
On page 16, line 13, immediately before "this", insert "titles I, II, and III of".
On page 18, line 3, immediately before "this", insert "title I, II, or III of".
On page 18, line 14, immediately before "this", insert "title I, II, or III of".
On page 18, line 23, immediately before "this", insert "titles I, II, or III of".
On page 19, line 1, immediately before "this", insert "title I, II, or III of".
On page 19, line 21, immediately before "this", insert "title I, II, or III of".
On page 20, line 2, immediately after "Act" insert "(other than title IV)".
On page 20, line 6, immediately before "this" insert "titles I, II, and III of".

Mr. ERVIN. Mr. President, will the Senator yield for a unanimous-consent request?

Mr. NELSON. I yield.

Mr. ERVIN. I ask unanimous consent that Brian Conboy, an aide to Senator Javits, and Barbara Dixon, an aide to Senator Bayh, have the privilege of the floor during the consideration of the pending measure.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. PERCY. Mr. President, I have an inquiry of the distinguished Senator from Wisconsin. We did go a little out of order in order to accommodate the schedule of the Senator from Maine (Mr. Muskie). We have not finished our opening statements yet. Unless the Senator has a time problem himself, I would like to complete our opening statements so we can proceed in an orderly manner, and I had indicated that I would yield to the Senator from Arizona (Mr. Goldwater) immediately after that, to present an amendment.

Mr. NELSON. My reason for calling up this amendment now is that the Senator from Maine (Mr. Muskie) will participate in a brief colloquy in connection with it.

Mr. PERCY. Does the Senator have any idea how long that brief colloquy may take?

Mr. NELSON. Just a few minutes. Senator Jackson has a brief statement. I will submit my statement for the Record.

Mr. President, I have a modification of the amendment as printed, I withdraw the amendment that is at the desk, and submit a clean copy that modifies that amendment. I ask for the immediate consideration of the amendment as modified.

Mr. Nelson's amendment No. 1945, as modified, is as follows:

At the end of the bill, add the following new title:

"TITLE IV—JOINT COMMITTEE ON GOVERNMENT SURVEILLANCE AND INDIVIDUAL RIGHTS

"ESTABLISHMENT

"SEC. 401 (a) There is hereby established a Joint Committee on Government Surveillance and Individual Rights (hereinafter referred to as the "joint committee") which shall be composed of sixteen members appointed as follows:

"(1) eight Members of the Senate, four to be appointed by the majority leader of the Senate and four to be appointed by the minority leader of the Senate; and

"(2) eight Members of the House of Representatives, four to be appointed by the majority leader of the House of Representatives and four to be appointed by the minority leader of the House of Representatives.

"(b) The joint committee shall select a chairman and a vice chairman from among its members.

"(c) Vacancies in the membership of the joint committee shall not affect the power of the remaining members to execute the functions of the join committee and shall be filed in the same manner as in the case of the original appointment.

"FUNCTIONS

"SEC. 402. (a) It shall be the function of the joint committee—

"(1) to make a continuing study of the extent and the method of investigation or surveillance of individuals by any department, agency, or independent establishment of the United States Government as such investigation or surveillance relates to the right to privacy, the authority for, and the need for such investigation or surveillance, and the standards and guidelines used to protect the right to privacy and other constitutional rights of individuals;

"(2) to make a continuing study of the intergovernmental relationship between the United States and the States insofar as that relationship involved the area of investigation or surveillance of individuals; and

"(3) as a guide to the several committees of the Congress dealing with legislation with respect to the activities of the United States Government involving the area of surveillance, to file reports at least annually and at such other times as the joint committee deems appropriate, with the Senate and the House of Representatives, containing its findings and recommendations with respect to the matters under study by the joint committee, and, from time to time, to make such other reports and recommendations to the Senate and the House of Representatives as it deems advisable; except that nothing in the foregoing provisions shall authorize the joint committee, or any subcommittee thereof, to examine lawful investigative or surveillance activities related to the defense or national security of the United States conducted within the territorial boundaries of the United States. For purposes of this subsection, lawful investigative or surveillance activities related to the defense or national security of the United States means investigative or surveillance activities carried on by duly authorized agencies to obtain information concerning unlawful activities directed against the Government of the United States which are substantially financed by, directed by, or otherwise involving the direct collaboration of foreign powers.

"(b) Nothing in this title shall give the joint committee, or any subcommittee thereof, jurisdiction to examine any activities of agencies and the departments of the United States Government conducted outside the territorial boundaries of the United States.

"REPORTS BY AGENCIES

"SEC. 403. In carrying out its functions, the joint committee shall, at least each year, receive, subject to the exceptions provided for in sections 402(a)(3) and 402(b), the testimony, under oath, of a representative of every department, agency, instrumentality or other entity of the Federal Government, which engages in investigations or surveillance of individuals, such testimony to relate to

"(a) the full scope and nature of the respective department's, agency's, instrumentality's, or other entity's investigations or surveillance of individuals; and

"(b) the criteria, standards, guidelines or other general basis utilized by each such department, agency, instrumentality or other entity in determining whether or not investigative or surveillance activities carried out or being carried out by such department, agency, instrumentality, or other entity were or are related to the defense or national security of the United States and thus within the purview of the exception provided for in such sections 402(a)(3) and 402(b).

"POWERS

"SEC. 404. (a) The joint committee, or any subcommittee thereof, is authorized, in its discretion (1) to make expenditures, (2) to employ personnel, (3) to adopt rules respecting its organization and procedures, (4) to hold hearings, (5) to sit and act at any time or place, (6) to subpena witnesses and documents, (7) with the prior consent of the agency concerned, to use on a reimbursable basis the services of personnel, information, and facilities of any such agency, (8) to procure printing and binding, (9) to procure the temporary services (not in excess of one year) or intermittent services of individual consultants, or organizations thereof, and to provide assistance for the training of its professional staff, in the same manner and under the same conditions as a standing committee of the Senate may procure such services and provide such assistance under subsections (i) and (j), respectively, of section 202 of the Legislative Reorganization Act of 1946, and (10) to take depositions and other testimony. No rule shall be adopted by the joint committee under clause (3) providing that a finding, statement, recommendation, or report may be made by other than a majority of the members of the joint committee then holding office.

"(b)(1) Subpenas may be issued under the signature of the chairman of the committee or of any subcommittee, or by any member designated by such chairman, when authorized by a majority of the members of such committee, or subcommittee and may be served by any person designated by any such chairman or member.

"(2) Each subpena shall contain a statement of the committee resolution authorizing the particular investigation with respect to which the witness is summoned to testify or to produce papers, and shall contain a statement notifying the witness that if he desires a conference with a representative of the committee prior to the date of the hearing, he may call or write to counsel of the committee.

"(3) Witnesses shall be subpenaed at a reasonably sufficient time in advance of any hearing in order to give the witness an opportunity to prepare for the hearing and to employ counsel, should he so desire. The chairman of the joint committee or any member thereof may administer oaths to witnesses.

"(c) The expenses of the joint committee shall be paid from the contingent fund of the Senate from funds appropriated for the joint committee upon vouchers signed by the chairman of the joint committee or by any member of the joint committee authorized by the chairman.

"(d) Members of the joint committee, and its personnel, experts, and consultants, while traveling on official business for the joint committee within or outside the United States, may receive either the per diem allowance authorized to be paid to Members of the Congress or its employees, or their actual and necessary expenses if any itemized statement of such expenses is attached to the voucher.

"(e)(1) The District Court of the United States for the District of Columbia shall have original jurisdiction, without regard to the sum or value of the matter in controversy, of any civil action heretofore or hereafter brought by the joint committee to enforce or secure a declaration concerning the validity of any subpena heretofore or hereafter brought by the joint committee, and the said District Court shall have jurisdiction to enter any such judgment or decree in any such civil action as may be necessary or appropriate to enforce obedience to any such subpena.

"(2) The joint committee shall have authority to prosecute in its own name or in the name of the United States in the District Court of the United States for the District of Columbia any civil action heretofore or hereafter brought by the joint committee to enforce or secure a declaration concerning the validity of any subpena heretofore or hereafter issued by such committee, and pray the said district court to enter such judgment or decree in said civil action as may be necessary or appropriate to enforce any such subpena.

"(3) The joint committee may be represented by such attorneys as it may designate in any action prosecuted by such committee under this title."

"DISCLAIMER

"SEC. 405. The provisions of this title shall not in any way limit or otherwise interfere with the jurisdiction or powers of any committee of the Senate, or the House of Representatives, or of Congress to request or require testimony or the submission of information from any representative of any department, agency, instrumentality or other entity of the Federal Government.

On page 3, line 23, after "Act", insert "(other than title IV)".
On page 4, line 6, after "Act", insert "(other than title IV)".
On page 6, line 9, immediately after "of", insert "titles I, II, and III of".
On page 6, line 12, after "under", insert "titles I, II, and III of".
On page 7, line 1, immediately before "this", insert "titles I, II, and III of".
On page 7, line 2, immediately before "this", insert "title I, II or III of".
On page 12, line 9, immediately before "this", insert "title I, II or III of".
On page 16, line 13, immediately before "this", insert "title I, II or III of".
On page 18, line 3, immediately before "this", insert "title I, II, or III of".
On page 18, line 14, immediately before "this", insert "title I, II, or III of".
On page 18, line 23, immediately before "this", insert "titles I, II or III of".
On page 19, line 1, immediately before "this", insert I, II, or III of".
On page 19, line 21, immediately before "this", insert "title I, II, or III of".
On page 20, line 2, immediately after "Act" insert "(other than title IV)".
On page 20, line 6, immediately before "this" insert "titles I, II, and III of".

Mr. NELSON. Mr. President, last November, the Senator from Washington (Mr. JACKSON) and I introduced legislation to create a joint committee of the Senate and the House of Representatives to provide legislative oversight over the surveillance activities of all the various agencies of the Federal Government, including the FBI, military intelligence, and the IRS.

The purpose, of course, is quite obvious: there is great potential for abuse of authority and invasions of privacy, which we have seen extensively engaged in in recent years, and Congress at present has no effective way to maintain a continuing oversight function to determine whether agencies were abusing their power and whether there need to be modifications or changes in current law.

The principal function of this joint committee would be to require that these respective agencies appear before the joint committee in public session or executive session when necessary, under whatever procedures would be established by that joint committee, and that the representatives of these agencies, such as the FBI, be put under oath, bring their records, show the committee what surveillance activities they have engaged in. For example, the FBI would show what wiretaps they have used, and whether the wiretaps in fact were secured pursuant to law, particularly the fourth amendment, which requires that searches and seizures are authorized only upon presentation of probable cause to an appropriate court, which may then issue the warrant.

Unless we bring these activities under congressional supervision, then, of course, the opportunities exist, as they have in the past, for very serious invasions of privacy of individuals, and freedom itself is endangered.

That, therefore, is the purpose of this amendment: to create this kind of a joint committee, with the authority which I have previously mentioned.

Hearings were conducted on the measure by the distinguished Senator from Maine (Mr. Muskie). Those proceedings have not all been completed.

Senator Jackson and I offered this as an amendment to the bill offered by the distinguished Senator from North Carolina (Mr. Ervin) some time ago because we thought it urgent and timely that this issue be raised, debated, and voted upon because we believe that Congress has to oversee Government surveillance activities on a continuing basis.

However, we have no desire to impair the possibilities of the adoption of the very fine piece of legislation that was designed by the distinguished Senator from North Carolina, and since it is now late in the session, the adoption of this amendment may very well cause the downfall of the whole bill.

If it were some time back, with plenty of room to maneuver in in terms of time, I would want to have the full debate and a rollcall vote.

I know that the distinguised Senator from North Carolina, as we all do, has been a leader in this whole field of protecting individual rights, especially the rights of privacy and other constitutional rights, and that he agrees certainly with the principle of the bill, although I have not asked him about the details. But Senator Jackson and I did not want to, in any way, jeopardize the possibilities of the adoption of his measure.

I would therefore like to ask the distinguished Senator from Maine if he might be able to advise us what his future plans would be in his committee for consideration of this particular subject matter.

Mr. MUSKIE. I would be delighted to do so.

First I compliment the distinguished Senator from Wisconsin and the distinguished Senator from Washington for their concern in the subject. It is one, I think, that is of increasing interest to Members of Congress and to the Members generally. It is deserving of the most extensive and comprehensive kinds of hearings.

Already we have had 6 days of hearings in the Government Operations Committee on national security secrecy, and the distinguished Senator from Wisconsin, as a matter of fact, testified at those hearings on his bill.

But we proceed from here. There are before us the Nelson-Jackson bill, to which the Senator is addressing himself, the Baker-Weicker bill on the same subject, and the Mathias-Mansfield resolution to have a study committee on oversight.

All of these have been referred to my subcommittee, and we will hold hearings and, I think, it is reasonably certain that the hearings will begin on December 9 and 10 of this year. There may be further hearings in addition to those, but I am committed to those, and I assure the Senator that we will pursue those hearings and the subject until the committee is in position to form some judgments.

Mr. President, more than 20 years ago, Supreme Court Justice Felix Frankfurter described the evolution of tyrannical power in the executive branch:

> The accretion of dangerous power does not come in a day. It does come, however slowly, from the generative force of unchecked disregard of the restrictions that fence in even the most disinterested assertion of authority.

Unfortunately, Justice Frankfurter's observation does much to explain why individual liberty has been eroded by an expanding web of snooping conducted at all levels of government. For many years now, the Government has used both simple and sophisticated techniques

to exercise almost unlimited power over the individual. The Government installs wiretaps, plants electronic bugs, uses computerized information to assemble dossiers on individuals, and engages in other surveillance activities which make a mockery of the individual freedoms guaranteed by our Constitution.

The dangers of uncontrolled Government surveillance were exposed again only this past week. The Justice Department released a report detailing the "cointelpro" program—the FBI's secret surveillance and disruption of organizations which the FBI considered to be a threat. These organizations included the Urban League, the Southern Christian Leadership Conference, the Congress on Racial Equality and other politically active groups. It was not shown that the individual members of these organizations were violating the law, and the FBI did not seek or receive the approval of the Attorney General or the President. Acting entirely on its own, the FBI engaged in these activities between 1956 and 1971. They were terminated when the "Media Papers" publicly exposed some of the FBI activities in 1971. And it was understandable why such public exposure would be a deterrent. The Justice Department's study called some of those activities "abhorrent to a free society," and for good reason. These activities included sending false and anonymous letters to discredit selected individuals in the eyes of their peers, informing an employer of the individual's membership in a particular group so that the individual might be fired, and passing on information to credit bureaus to harm the individual economically.

Mr. NELSON. I appreciate the comments of the Senator from Maine. I also know, as we all do, of his concern about individual rights and constitutional rights, and I know that the measure is in good hands in his committee and that he recognizes the importance of Congress doing something about managing this problem that has arisen and received so much publicity in recent years.

These revelations concerning the FBI coincided with other revelations concerning the surveillance activities of the Internal Revenue Service. According to recently disclosed documents, the IRS—acting at the behest of the White House—monitored the tax records and political activities of 3,000 groups and 8,000 individuals between 1969 and 1973. The groups monitored included the Urban League, Americans for Democratic Action, the National Student Association, the Unitarian Society and the National Council of Churches. These IRS activities did not reflect a neutral enforcement of the tax laws; they represented instead a blatant attempt to secure private information about the politics of people whose views did not coincide with those of the White House. Indeed, these secret activities were continued for four years despite the fact that there was little information to show violation of the tax laws.

These FBI and IRS actions, as well as other surveillance activities, make clear the need for congressional controls of Government spying. To this end, Senator Jackson and I are introducing an amendment to S. 3418 which would establish a bipartisan joint committee of Congress to oversee all Government surveillance activities. At least once each year, representatives of the FBI, the IRS, and every Governmental agency that engages in surveillance would be required to testify before the joint committee under oath about the full scope and nature of

their respective agency's spying activities. The joint committee, moreover, would be entitled to all relevant information concerning those activities and practices. There is only one narrowly defined exception to the committee's broad jurisdiction over Government surveillance: those cases directly involving foreign powers who are engaged in unlawful activities which endanger this country's security. However, the committee would be explicitly directed to obtain information from the Government concerning the criteria used to determine whether an activity qualifies under the exception. This, in turn, would help insure that the exception is not misused or interpreted too broadly.

As part of its responsibilities; the joint committee would be obligated to report to the full Congress as often as it deems necessary, but in any event, at least once a year. The report would include the committee's findings as to whether the Government is complying fully with the law, whether the courts are exercising their review powers diligently, and whether additional legislation is needed to protect the right to privacy and other fundamental liberties from Government snooping.

The need for this continuing and comprehensive congressional oversight is beyond question. The FBI and IRS activities I cited earlier are not isolated incidents. Indeed, other examples make clear that there is an incredibly broad system of Government surveillance which can and often does escape congressional scrutiny. Among these examples are the following:

In 1970, President Nixon approved the "Huston Plan," an interagency scheme for domestic surveillance which provided for the use of wiretaps, electronic bugs, break-ins and other activities which a staff assistant described as "clearly illegal." Although the plan was revoked five days later, because of the objections by FBI Director Hoover, President Nixon's continued interest in the idea ultimately led to the creation of the "Plumbers," a White House unit which carried out the break-in at Daniel Ellsberg's psychiatrist's office and engaged in other questionable surveillance activities. Indeed, one recent article reported that there had been at least 100 illegal break-ins conducted by the "plumbers" and other secret Government units.

A 1973 Senate subcommittee report detailed the extensive spying secretly conducted by 1,500 agents of the U.S. Army on more than 100,000 civilians in the late 1960's. This surveillance was directed principally at those suspected of engaging in political dissent. No one in the Congress knew about this spying. No one in the executive branch would accept responsibility for it. Again, there is no guarantee that this sorry episode will not be repeated. In fact, a Senate committee learned recently that in the last 3 years—after the administration assured the public that the military would no longer spy on civilians—the U.S. Army has maintained numerous surveillance operations on civilians in the United States. And an article in the New Republic magazine of March 30, 1974, detailed the U.S. Army's use of wiretaps, infiltrators, and other surveillance techniques to spy on American citizens living abroad who supported the Presidential candidacy of George McGovern. The Army's spying was reportedly so extensive that it even intercepted a letter from a college librarian in South Carolina who requested information about a German publication.

On April 14, 1971, it was revealed that the FBI had conducted general surveillance of those who participated in the Earth Day celebrations in 1970. These celebrations involved tens of thousands of citizens, State officials, representatives of the Nixon administration, and Members of Congress. As the one who planned that first Earth Day, I cannot imagine any valid reason for spying on individuals exercising their constitutional rights of speech and assembly in a peaceable manner. There is still no satisfactory explanation of the surveillance. Nor is there any guarantee it will not be repeated in the future.

Innumerable Government officials, including President Lyndon Johnson, Supreme Court Justice William O. Douglas, Congressman Hale Boggs, and Secretary of State Henry Kissinger, believed that their private telephones had been secretly wiretapped. These concerns coincide with known facts regarding other citizens. In May 1969, for example, the White House secretly authorized wiretaps on 17 Government officials and newspapermen without first obtaining an approving judicial warrant. The purported basis of these "taps" was a concern that these individuals were involved in "leaks" of sensitive information. The Government allegedly believed that publication of this information did or would jeopardize "national security." There is still no public evidence to justify that belief. Indeed, there is no public evidence to demonstrate that all of the individuals tapped even had access to the information leaked.

The Justice Department still maintains a practice of installing warrantless wiretaps on American citizens and others when it feels "national security" is involved. This practice violates the plain language of the fourth amendment—which requires a judicial warrant based on probable cause before the Government can invade an individual's privacy. There is no public information concerning the number of warrantless wiretaps installed in the last year or presently maintained. Incredibly enough, the Department has refused to provide this information—even in executive session—to legislative subcommittees of the House and Senate. However, it is known that some of these wiretaps were authorized even though there was no direct collaboration of a foreign power. The tap installed on newspaper columnist Joseph Kraft's home telephone is perhaps the best known example. Under our proposal, the joint committee would be required to interrogate Government officials about "national security" wiretapping and uncover the actual criteria used by the Government in determining that a foreign power is directly involved.

The Senate Watergate and Senate Judiciary Committees received evidence that in 1969 the White House established a special unit in the Internal Revenue Service to provide the administration with secret access to the confidential tax records of thousands of its "enemies." The dissemination of these private records was so flagrant and so widespread that one investigating Senator likened the IRS to a public lending library.

These examples are only the tip of the iceberg. As early as 1967, Prof. Alan Westin reported in his book, "Privacy and Freedom," that:

> At least fifty different federal agencies have substantial investigative and enforcement functions, providing a corps of more than 20,000 "investigators" working for agencies such as the FBI, Naval Intelligence, the Post Office, the

Narcotics Bureau of the Treasury, the Securities and Exchange Commission, the Internal Revenue Service, the Food and Drug Administration, the State Department, and the Civil Service Commission. While all executive agencies are under federal law and executive regulation, the factual reality is that each agency and department has wide day-to-day discretion over the investigative practices of its officials.

The numbers—and dangers—of this official spying have surely increased since 1967. But even those 1967 figures, as well as the examples I have described, should be more than sufficient to demonstrate what should be clear to everyone: uncontrolled Government snooping is a dangerous assault on our constitutional liberties. Those liberties are the cornerstone of our democratic system and any assault on them cannot be treated lightly. A society cannot remain free and tolerate a Government which can invade an individual's privacy at will.

Government snooping is particularly dangerous because often it is executed without the knowledge or approval of those officials who are accountable to the public. This, in turn, increases the probability that Government invasions of individual privacy, as well as other fundamental constitutional liberties, will be accomplished by illicit means and for illegitimate purposes.

The FBI's "cointelpro" activities are a clear illustration of the problem. Another example is the break-in of Daniel Ellsberg's psychiatrist's office. This illegal act was perpetrated in September 1971 by members of the "plumbers," a special unit established within the White House and ultimately accountable to the President himself. After the break-in was publicly exposed, the "plumbers" claimed that they were acting under the explicit authority of the President in an effort to protect "national security." But available public evidence suggests that Mr. Nixon did not give his approval to the break-in. Indeed, the White House transcripts indicate that President Nixon did not learn of the break-in until March 1973—18 months after it occurred. In short, a blatant criminal act—which included the violation of one doctor's privacy—was perpetrated by Government agents and those with ultimate responsibility had no procedure to stop it.

The central question is how many other incidents of illegal spying by the Government remain undisclosed? And how many more such incidents must be disclosed before Congress recognizes the need for immediate action?

There is no question, however, that those sensitive to civil liberties have long understood the need for congressional action to end the dangers of Government snooping. As early as 1971 I introduced legislation for that purpose. Now the public at large has also awakened to the need for legislation to protect their rights against Government snooping. Numerous opinion polls indicate that the people's principal concern today is the preservation of their freedom—freedom which is too easily and too often taken for granted. These polls, including some conducted by Louis Harris, have made the following findings:

Fifty-two percent of the public believes that "things have become more repressive in this country in the past few years;"

Seventy-five percent of the public believes that "wiretrapping and spying under the excuse of national security is a serious threat to people's privacy;"

Seventy-seven percent of the public believes Congress should enact legislation to curb government wiretapping;

Seventy-three percent of the public believes Congress should make political spying a major offense.

On the basis of these and other findings, pollster Harris drew two basic conclusions. First, "government secrecy can no longer be excused as an operational necessity, since it can exclude the participation of the people in their own government, and, indeed, can be used as a screen for subverting their freedom." Second, "the key to any kind of successful future leadership must be iron bound integrity."

The message of these opinion polls is clear: Congress must enact legislation to end abusive government surveillance practices which violate the fundamental rights and liberties guaranteed by our Constitution. The government should not be able to use wiretaps and other electronic devices to eavesdrop on citizens for "national security" purposes when there is no involvement of a foreign power and no judicial warrant. The Government should not be able to use income tax returns and other computerized, confidential information for political purposes. The Government should not be able to conceal its illicit activities by invoking the "separation of powers" or the need for secrecy. In a word, the Government should not be able to escape its obligation to the Constitution and the rule of law. Otherwise, we shall find that unrestrained Government power has replaced individual liberty as the hallmark of our society.

One does not have to attribute malevolent motives to government officials in order to realize the need for congressional action. Good intentions are not the criteria for judging the lawfulness of propriety of Government action. In fact, the best of intentions often produce the greatest dangers to individual liberty. As Supreme Court Justice Brandeis once observed:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficient. Men born to freedom are naturally alert to repel invasions of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Relying on this historical judgment, the Supreme Court held in the 1972 *Keith* case that the Government cannot wiretap American citizens for "domestic security" purposes without court authorization. In issuing this decision, the court declared, as a matter of constitutional law, that the Government's self-discipline is inadequate to protect the individual freedoms guaranteed by the fourth amendment. The Court's judgment was not premised on the malicious dispositions of those who inhabit the executive branch. Rather, the judgment flowed from the conflicting interests which the Government is required to serve. Speaking for a unanimous Court, Justice Lewis Powell examined the evolution and contours of the freedoms protected by the fourth amendment. He then stated:

> These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the executive branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility is to enforce the laws, to investigate and to prosecute. . . . The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressure to obtain incriminating evidence and overlook potential invasion of privacy and protected speech.

In this context, a congressional oversight committee would be a two-edged sword in the effort to end the abuses of Government snooping.

On the one hand, this committee could provide assurances to the public that Government surveillance activities are limited to those conducted by lawful means and for legitimate purposes. On the other hand, the oversight committee could help the executive branch to insure that Government agents do not misuse the public authority entrusted to them. Fulfillment of these two functions by the oversight committee would do much to eliminate illegal and unethical Government spying.

In considering creation of a congressional oversight committee, Congress should not yield to self-serving assertions by the executive branch that the power to investigate and conduct surveillance to investigate and conduct surveillance is exclusively within its jurisdiction and that Congress has no right to sensitive information concerning such investigations and surveillance activities. This argument is nonsense. Certainly there is no language in the Constitution which allows Government surveillance activities to escape congressional scrutiny. Indeed, such an escape clause would be at odds with the fundamental premise of our constitutional system that all power is "fenced about," that every coordinate branch of Government is subject to the check of the other branches. If Government investigative and surveillance activities can be maintained by Government secrecy, there would be no way for the Congress to know whether it should exercise its power to check the executive branch.

Moreover, a lack of congressional oversight would cripple Congress ability to protect those individual freedoms guaranteed to everyone by the Constitution. In the Federalist Papers, James Madison acknowledged Congress as "the confidential guardians of the rights and liberties of the people." Congress cannot fulfill its responsibility to protect those rights and liberties unless it first has the facts concerning the scope and nature of Government investigative and surveillance activities. Access to those facts is also important if Congress is to exercise its other responsibilities. Thus, the Constitution empowers Congress—not the President—to regulate interstate commerce: the Constitution empowers Congress—not the President—to appropriate public moneys for Government operations, including investigative and surveillance activities: the Constitution empowers Congress—not the President—to enact laws concerning the punishment of criminal offenses and the protection of individual privacy. Having been granted these powers, the Congress should obtain the information necessary to insure that they are exercised wisely.

The need for this congressional oversight committee, then, should not be underestimated. The individual's right to privacy is one of our most cherished liberties. It is fundamental to the concept of democratic self-government where each individual's private thoughts and beliefs are beyond the reach of Government. Without that right to privacy, the individual's freedom to participate in and guide his Government is jeopardized. Government then becomes a monster to be feared rather than a servant to be trusted.

As Justice Stephen Field stated in 1883:

> Of all the rights of the citizens, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves not merely protection of his person from assault, but exemption of his private affairs, books and papers from the scrutiny of others. Without enjoyment of this right all others would lose half their value.

A right so vital to individual liberty and, indeed, to our constitutional system deserves rigorous protection by Congress—the people's chosen representatives. The amendment being offered today provides a timely opportunity to establish that protection and assure the American public that individual freedom is still the foundation of our political system.

Mr. JACKSON. Mr. President, last November Senator Nelson and I introduced S. 2738 to establish a watchdog joint congressional committee to oversee activities of the Federal Government affecting the right to privacy of all American citizens. Our purpose was to create and focus in one congressional committee the responsibility for overseeing domestic surveillance and investigative activities of Federal agencies as those activities relate to the need to protect and defend individual privacy and freedom for all American citizens from serious and destructive erosion. Today I am pleased to join with Senator Nelson to offer a modified version of this legislation as an amendment to S. 3418, a bill to create a Federal Privacy Commission to monitor and regulate data banks.

Individual privacy and freedom, which are at the heart of our system of democratic self-government, are under severe pressure today. Modern technology has vastly increased the ease with which intrusions on individual privacy may be conducted. By 1967 over 50 Federal agencies were engaged in investigative activities employing over 20,000 investigators. These included such diverse agencies as the Food and Drug Administration, the Securities and Exchange Commission, the Treasury Department, the Justice Department, and many others. Since that time the number of agencies and investigators has almost certainly increased and it has become clear to the American people that there is a danger that the power of the Federal Government may be abused to indiscriminately employ modern techniques of surveillance for illegitimate purposes or by unregulated procedures. This danger represents a serious threat to the integrity of individual rights and, therefore, to our entire way of life in America.

The American people are deeply disturbed about evidence that has accumulated in recent years of widespread Government insensitivity and disregard for the rights of individual citizens. Watergate and related scandals have brought to light a callous disregard for the law and for the sanctity of individual rights within the highest circles of government. Such activities as the formation of the "Plumbers" for the purpose of carrying on internal security operations which included wiretapping and burglary smacks of a secret police operation that has no place in American life.

Over the past week there have been new revelations that Government agencies have engaged in secret intelligence gathering and "dirty tricks" operations aimed at political and activist organizations. These revelations have further shaken the confidence of the American people in the integrity and methods of Federal investigative agencies.

A lawsuit filed by a public interest law firm brought the disclosure that a secret unit within the IRS named the "Special Service Staff" began gathering intelligence in the summer of 1969 as a result of direct White House pressure. The Special Service Staff unit collected intelligence and investigated 99 political and activist organizations and was

not disbanded until after the Watergate scandals became public. The use of the IRS to perform unauthorized law enforcement type functions for essentially political purposes is a flagrant and inexcusable abuse of power. This action undermines public confidence which is absolutely essential if the IRS is to perform its job of administering the tax laws. More importantly, it runs counter to fundamental values of freedom of expression and equal treatment under the law to have an agency of Government collecting data to be used against organizations with political views that are not favored by the current administration.

The purpose of the Joint Committee which Senator Nelson and I have suggested would be to assure public accountability of Federal investigative agencies by assuring better congressional oversight of their activities. As was noted editorially in the Washington Star on November 20:

> It is imperative that Congress begin exercising much closer oversight of operations for which it provides the legal basis and the financing. It should not be left to high-level bureaucrats, especially in the agencies with awesome investigative authority, nor to White House politicians to decide what is or is not good for the people and then use highly questionably means to exercise that which they consider bad.

I firmly believe that the Congress does bear a heavy responsibility to assure that Federal investigative agencies do not disregard the civil liberties of the American people. The legislation which Senator Nelson and I have suggested will give us the tools to do this job.

Senseless violations of individual rights have occurred, in part, because we in the Congress have not pursued with sufficient vigor our responsibility to closely oversee the activities of the innumerable Federal agencies which have an impact on the right to privacy of millions of Americans. As a result, the American people are very much concerned about the need for increased efforts to protect our cherished tradition of individual liberty in the wake of disclosures of such blatant abuses. Recent polls indicate that 75 to 80 percent of the American people favor tough new laws making unlawful wiretapping a major criminal offense.

I am pleased that the Congress has begun to respond to the need for legislation designed to better protect individual rights. S. 3418 is an important bill which will do a great deal to assure the right to privacy for millions of Americans about whom the Federal Government has collected and maintains records in computer data banks. For this reason, I have been active in the development and joined as a cosponsor of this legislation.

I believe the amendment that Senator Nelson and I are now offering would strengthen and broaden the scope of S. 3418 by addressing the equally important issue of regulating and overseeing the activities of Federal investigative agencies. The committee we are suggesting would be invaluable as a means of focusing and improving congressional oversight of Federal agencies to assure that they do not overstep their statutory and constitutional authority in ways that have an adverse impact on individual freedom. At present, 12 or more congressional committees oversee the activities of the uncounted but innumerable Federal agencies which conduct investigative activities. The comprehensive overview of these agencies that would be provided by our legislation would provide a more effective safeguard against the use of in-

vestigative and surveillance powers in ways that fly in the face of our traditional commitment to personal freedom and liberty.

I am pleased that Senator Muskie will hold hearings on this amendment on the 9th and 10th of December.

Mr. ERVIN. Mr. President, will the Senator from Wisconsin yield?

Mr. NELSON. I yield to the Senator.

Mr. ERVIN. I thank the Senator for his very complimentary statement of my work in the field of individual rights. I have always had the aid of the distinguished Senator from Wisconsin on that, and I am proud to be, along with him and one or two other Members of the Senate, one of the authors of the bill to repeal the no-knock law.

I wish to commend his action in this matter and the action of the distinguished Senator from Maine. I think that is the proper course to take because if we sometimes put too big a load on one little legislative nag he has a hard time making the journey to his ultimate destination.

I thank the Senator for his course of action and the Senator from Maine for giving the assurance that he will hold hearings on the proposal which, I think, deserves wise and careful thought.

Mr. NELSON. I thank the Senator from North Carolina. I only regret that he has decided voluntarily not to join us again in the next session because I think that about 90 percent of the influence I have on this kind of an issue is as a result of my association with the Senator from North Carolina, which I now lose.

Mr. WEICKER. If the Senator from Wisconsin will yield for one moment. I commend the Senator from Wisconsin and the Senator from Washington for their legislation.

I want to thank the distinguished Senator from Maine for proposing hearings on this bill, and also on the bill proposed by Senator Baker and myself.

As each week goes by and more of these abuses come to the public's knowledge, I think it is terribly important that we act. We all realize the difficulties that this type of legislation, the type proposed by Senator Nelson and Senator Baker, have had in the past. But it has got to be clear to this body that nobody has been taking responsibility for any oversight relative to these various agencies.

We owe it to the public now to take this entire area of law enforcement and intelligence gathering and make it accountable to the people of the United States through their elected representatives.

I would hope that we not only have the hearings but also we make this one of the first orders of business for Congress in the months ahead.

I thank the Senator from Wisconsin.

Mr. NELSON. I thank the Senator.

I yield the floor.

The PRESIDING OFFICER. The question is on agreeing to the amendment of the Senator from Wisconsin.

Mr. NELSON. Mr. President, I withdraw my amendment.

The PRESIDING OFFICER. The Senator's amendment is withdrawn.

Mr. GOLDWATER. Mr. President, by a happy coincidence, the House at this very moment is considering almost identical legislation to this, legislation introduced by my son who represents the 20th District of California.

Mr. President, I am very happy to be a cosponsor of this legislation and happy to have introduced a piece of legislation quite similar to it.

Mr. President, I am proud to rise today in support of the committee bill to protect individual privacy in the collection and use of personal data by Federal agencies.

Mr. President, the need for protection of personal privacy has come to the fore only in recent years, although its source is found in the Constitution itself.

Reports uniformly calling for the adoption of safeguards for the fair storing and handling of personal information have been published by the Departments of Communications and Justice in Canada in 1971, the Younger Committee on Privacy in Great Britain in 1972, the International Commission of Jurists in 1972, the National Academy of Sciences Project on Computer Databanks, also in 1972, and the Secretary's Advisory Committee on Automated Personal Data Systems of the Department of Health, Education, and Welfare in 1973.

In late 1973, legislation was introduced in the House of Representatives (H.R. 10042) by Congressman Goldwater, Jr., and in the Senate (S. 2810) by me, to implement the common principles shared by these various studies. I believe the committee bill before us today includes these same safeguards insofar as the operations of Federal agencies and departments are concerned. The basic safeguards are:

First. There must be no personal data system whose very existence is secret.

Second. There must be a way for an individual to find out what information about him is in a record and how that information is to be used.

Third. There must be a way for an individual to correct information about him, if it is erroneous.

Fourth. There must be a record kept of every significant access to any personal data in the system, including the identity of all persons and organizations to whom access has been given.

Fifth. There must be a way for an individual to prevent information about him collected for one purpose from being used for other purposes, without his consent.

Mr. President, it is my belief that in order for the individual to truly exist, some reserve of privacy must be guaranteed to him. Privacy is vital for the flourishing of the individual personality and to "the imaginativeness and creativity of the society as a whole." So said the Report of the Committee on Privacy of Great Britain in 1972.

By privacy, Mr. President, I mean the great common law tradition that a person has a right not to be defamed whether it be by a machine or a person. I mean the right "to be let alone"—from intrusions by Big Brother in all his guises. I mean the right to be protected against disclosure of information given by an individual in circumstances of confidence, and against disclosure of irrelevant embarrassing facts relating to one's own private life, both rights having been included in the authoritative definition of privacy agreed upon by the International Commission of Jurists at its world conference of May, 1967.

By privacy, I also mean what the U.S. Supreme Court has referred to as the embodiment of "our respect for the inviolability of the human personality," and as a right which is "so rooted in the traditions and conscience of our people as to be ranked as fundamental."

What we must remember today is that privacy in the computer age must be planned. Privacy, as liberty, is all too easily lost. We must act now while there is still privacy to cherish.

AMENDMENT NO. 1914

Mr. GOLDWATER. Mr. President, I call up for myself and the senior Senator from Illinois (Mr. Percy), our amendment No. 1914, to halt the spread of the social security number as a universal population identifier.

The PRESIDING OFFICER. The clerk will report the amendment.

The assistant legislative clerk read as follows:

MORATORIUM ON USE OF SOCIAL SECURITY NUMBER

SEC. 307. (a) It shall be unlawful for—

(1) any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number, or

(2) any person to discriminate against any individual in the course of any business or commercial transaction or activity because of such individual's refusal to disclose his social security account number.

(b) The provisions of subsection (a) shall not apply with respect to—

(1) any disclosure which is required by Federal law, or

(2) any information system in existence and operating before January 1, 1975.

(c) Any Federal, State, or local government agency which requests an individual to disclose his social security account number, and any person who requests, in the course of any business or commercial transaction or activity, an individual to disclose his social security account number, shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

Mr. GOLDWATER. Mr. President, when parents cannot open bank accounts for their children without obtaining social security numbers for them; when all schoolchildren in many ninth grade classes are compelled to apply for social security numbers; when a World War I veteran is asked to furnish his social security number in order to enter a Veterans' Administration hospital; and when the account number is used and required for numerous other purposes totally unrelated to the original social security program; then I believe it is time for society to stop this drift toward reducing each person to a number.

There already have been issued a total of over 160 million social security numbers to living Americans. The total number issued in 1972 increased almost 50 percent over 1971, while the number issued to children age 10 and younger rose 100 percent.

There is no statute or regulation which prohibits, or limits, use of the account number. To the contrary, a directive issued by President Roosevelt 32 years ago, is still in effect requiring that any Federal agency which establishes a new system of personal identification must use the social security number.

Numerous Americans deplore this development. They resent being constantly asked or required to disclose their social security number in order to obtain benefits to which they are legally entitled. They sense that they are losing their identity as unique human beings and are being reduced to a digit in some bureaucratic file.

Scholars who have studied the situation have fears which run far deeper. These writers believe that the growing use of the social security number as a population number will brand us all as marked individuals.

What is meant is that when the social security number becomes a universal identifier, each person will leave a trail of personal data

behind him for all of his life which can be reassembled to confront him. Once we can be identified to the Administrator in government or in business by an exclusive number tied to each of our past activities—our travels, the kinds of library books we have checked out, the hotels we have stayed at, our education record, our magazine subscriptions, our health history, our credit and check transactions—we can be pinpointed wherever we are. We can be manipulated. We can be conditioned. And we can be coerced.

Mr. President, the use of the social security number as a method of national population numbering is inseparable from the rapid advances in the capabilities of computerized personal data equipment. The state of the art in computer data storage is now so advanced that the National Academy of Sciences reported in 1972:

> That it is technologically possible today, especially with recent advances in mass storage memories, to build a computerized, on-line file containing the compacted equivalent of 20 pages of typed information about the personal history and selected activities of every man, woman, and child in the United States, arranging the system so that any single record could be retrieved in about 30 seconds.

The concern I have about the spread of the social security identifier is also tied to the ravenous appetite of the Washington bureaucracy for information. A House Post Office and Civil Service Subcommittee reported in 1970 that Washington's paperwork files would fill 12 Empire State buildings stacked on top of each other. These files already include over 2 billion records traceable to personal individuals.

Where will it end? Will we allow every individual in the United States to be assigned a personal identification number for use in all his governmental and business activities? Will we permit all computerized systems to interlink nationwide so that every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution?

The time to think about the future is now. We must build into the law safeguards of human privacy while a national numbering system is not yet an accomplished fact. Accordingly, Senator Percy and I propose to place a moratorium on the use of social security numbers for purposes unrelated to the original program.

Our amendment will make it unlawful for any governmental body at the Federal, State, or local level to deny to any person a right, benefit, or privilege because the individual does not want to disclose his social security account number. The amendment also provides that it shall be unlawful for anyone to discriminate against another person in any business or commercial dealings because the person chooses not to disclose his account number.

The prohibitions of our amendment would take effect beginning on January 1, 1975. Any information system started after that date will be subject to the amendment, but any information system in existence before then is exempt.

Mr. President, medical and sociological evidence proves that the need for privacy is a basic, natural one, essential both to individual physical and mental health of each human being and to the creativity of society as a whole. The Supreme Court of the United States has stated on repeated occasions that personal privacy is also a fundamental right of U.S. citizenship, guaranteed by the Constitution to

every citizen. Mr. President, it is for us to determine today just how much privacy shall remain for the individual in the future, and I hope the Senate will act favorably upon both our amendment and the committee bill.

Mr. President, I ask unanimous consent that Senator HELMS' name be added as a cosponsor.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. PERCY. Will the Senator yield?

Mr. GOLDWATER. I yield to the Senator.

Mr. PERCY. Mr. President, I shall be very brief. Mr. President, it is a distinct pleasure to join Senator Goldwater, together with my esteemed colleague, Senator Ribicoff, who asked to be included as a co-sponsor of the pending amendment, in offering an amendment to limit use of the social security number. The senior Senator from Arizona is an acknowledged leader in the Senate on matters relating to the social security number and privacy. On the same matters, I have had long extended discussions with Congressman Barry Goldwater, Jr. from California, who is a principal author in the House of the privacy legislation shortly to be considered by that body.

I consider him to be vigilant defender of citizens' individual rights of privacy.

Our concern is that the social security number is fast becoming the single common identification number for each and every American citizen. For many years we have heard proposals to compel all school children of a certain grade level to receive a social security number. It has even been suggested that every newborn infant be labeled with such a number. To a great many Americans, the image of such a policy put into practice is abhorrent. Yet the problems surrounding the misuse of the social security number are more than symbolic of our new era of data banks and our fears of a centrally controlled Big Brother society.

In 23 States, it is impossible to vote in a local, State or even national election without first supplying a social security number. In the State of Virginia, for example, you cannot vote, register an automobile, or even obtain a driver's license unless you first disclose your social security number.

In West Virginia, it is required for fishing licenses. The Federal Reserve Board requires it to join their car pool. Senate wives once had to give it before entering the White House when visiting with Mrs. Nixon for tea. The social security number appears on every Senate staff member's identification card. The number is used widely throughout the Government, and it is even used as the principal identification number by the U.S. Army. All of these uses continue, and yet if you look at your own social security card, at the bottom, it reads,

For social security and tax purposes—not for identification.

The social security number was clearly not intended by its creators to become the universal identifier. But in the race to computerize every known fact stored by the Government about its citizens, the warning on our cards has been ignored. It is not so much that the social security number had to be used by the computer programmers and data collectors. It was there and it was convenient. Apparently no one gave thought 15 or 20 years ago to the possibility that massive computeriza-

tion of personal data files on the basis of a single unprotected number could someday pose a problem.

That lack of foresight was unfortunate—for now hundreds of Government computer systems and thousands of private computer systems use the social security number in the indexing and identification of individuals. The possibility is growing that anyone with access to the proper computer terminal could type in a social security number and thereby order the computer to print out details concerning what cars we own, and what our driving record is like, how we spend our money and how we pay our bills, how we did in school, what we tell our doctor and what he tells us in return.

The amendment that we offer is a modest proposal to limit the expansion of the use of the social security number. We recognize that we cannot yet justify a law requiring the reprogramming of massive computer systems maintained by the military, by universities, and by private employers. After careful consideration, we have determined that a moratorium ought to be placed on the ability of both Government and private organizations to develop new programs and new procedures that require an individual to furnish his social security number.

Under our amendment, Federal Government and private organizations that begin using the social security number after January 1, 1975, cannot deny a right, benefit, or privilege to an individual who refuses to disclose his number, unless the disclosure is required by Federal law. Furthermore, all requests by an organization of an individual for his social security number must be accompanied by the following information: whether disclosure is mandatory, what is the legal authority for the request, what uses will be made of the number, and what rules of confidentiality will apply.

Mr. President, these provisions directly reflect the specific recommendations of the oft-cited text "Records, Computers, and the Rights of Citizens," which was published in 1973 by the Secretary of HEW's Committee on Automated Personal Data Systems. The amendment is also consistent with the general position presented in the Social Security Administration's "1971 Task Force Report on the Social Security Number."

Our amendment overcomes the questions raised earlier by several of my colleagues. These questions centered around the disruption of established procedures and the uncertain but large cost involved in changing recordkeeping procedures nationwide. The amendment will not require redesigning forms and reprograming computers. It will not disrupt established procedures and it will not create unwarranted cost burdens, because it specifically exempts any disclosure of the social security number which is required by Federal law, or any use which is in existence and operation prior to January 1, 1975.

Mr. President, the amendment that we now propose is but a small tribute to the tireless efforts over many years by the most respected senior Senator from North Carolina, Senator Ervin, to beat down invasion of privacy on numerous fronts. Our amendment does not pretend to solve all of the problems raised by abuses of the social security number, but it will halt the unchecked spread of these abuses and bring us to a uniform national policy.

Mr. ERVIN. Will the Senator from Arizona yield?

Mr. GOLDWATER. I will be happy to yield.

Mr. ERVIN. I think the amendment offered by the Senator from Arizona, cosponsored by the distinguished Senator from Illinois, is very meritorious, and I hope the Senate will adopt it. I want to take this occasion to commend the Senator from Arizona for the good work he has done in supporting this entire legislation.

Mr. GOLDWATER. I thank the Senator.

Mr. HRUSKA. Mr. President, has the amendment been disposed of?

Mr. GOLDWATER. I was wondering if it had been disposed of.

The PRESIDING OFFICER. The amendment is still pending. The Chair was not certain whether the Senator from Nebraska wanted to address the amendment.

If not, the question is on the amendment of the Senator from Arizona (putting the question).

The amendment was agreed to.

The PRESIDING OFFICER. The Senator from Nebraska.

Mr. HRUSKA. Mr. President, I rise to address some questions and express some misgivings about the pending measure. It is a measure which seeks to establish a Federal privacy board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State and local governments, and other organizations, regarding such information, and for other purposes.

It seeks to gain these objectives, Mr. President, by granting very extensive powers and duties to the Privacy Commission which the legislation creates.

Mr. President, the general declared objectives of the bill are desirable and worthy. I support these objectives. There have been many abuses in the area of privacy with which this bill deals. Many past abuses have been identified and have been corrected. As new abuses of privacy appear, there have been good faith efforts by both the congressional and executive branch to remedy them.

But notwithstanding such efforts, there are still a number of areas in which great improvement can be made, to protect the privacy of individual data collected and maintained by the Government, by proper statutory authority and other regulatory efforts. There is little doubt that there is much room for improvement in the manner in which our Government treats the personal information of its citizens.

It is, however, Mr. President, the effectiveness, the propriety, and the wisdom of the form which this bill takes in order to safeguard personal information which raises some question.

While there are other observations which could be addressed to various specific provisions of the bill, I shall briefly refer only to two major aspects of the legislation in my present remarks.

One aspect has to do with the nature and scope of the duties and responsibilities of the Federal Privacy Commission provided for in the bill.

The second major aspect pertains to the inclusion of criminal justice and the law enforcement records and files within the purview of the legislation.

As to the first, Mr. President, it should be noted that the scope and range of activities permitted the board are very broad. The board

may concern itself not only with Federal agencies and offices, but also with organizations in the private sector, in State and regional government, and in charitable and political organizations.

Happily, it is excluded from examining religious organizations, but aside from that I doubt very much that any system of data gathering would escape the microscopic as well as the macroscopic eye of the Federal Privacy Commission.

Mr. President, the present law, together with many longstanding precedents, assigns oversight responsibilities regarding many of the Federal agencies and activities to the Congress. There are, for example, oversight powers, presently being exercised by the Committees on the Judiciary, in both bodies of Congress, dealing with the Federal Bureau of Investigation and its related information gathering activities.

Similarly, there are the Committees on Commerce in both bodies of Congress which concern themselves, and have for many decades with the regulatory bodies, such as the Interstate Commerce Commission, the Civil Aeronautics Board, and the Federal Trade Commission.

We also have the Committee on Finance in the Senate and the Ways and Means Committee in the House which concern themselves with the Internal Revenue Service and with the various activities that are lodged in the Treasury Department.

These are examples where, through the years—either by statute or by inherent constitutional powers—Congress has exercised oversight on Federal activities and agencies.

Normally when Congress seeks to delegate its powers and responsibilities it does so in a limited fashion. But here, Mr. President, under the terms of this bill, the Federal Privacy Board would be vested with vast responsibility and supervisory power.

Such a delegation of responsibility as is represented in this bill is a little at variance with what we like to see. This is because when we create powers in bodies of this kind Congress has generally tried to define in more or less precise language—preferably more precise—the bounds of such power.

Mr. President, the Board created by this act would supersede and impose itself upon all existent statutory, or actual, oversight and supervision of the various other agencies and activities that are involved. It would create another layer of Federal officials who would go abroad and interest themselves in getting into almost limitless numbers of activities and areas of human conduct in this country. It would indeed be far flung in its organization. It would have to be, of course, if it were going to be effective for its declared purposes. It would be armed with money and with penetrating powers—power to get witnesses and records in almost any public or private area in which it might care to interest itself.

Mr. President, it is respectfully suggested that this type of supervisory activity will tend to result in confusion and conflict and indecision. It may tend to diminish the immediate and direct interest of Congress in the exercise of its oversight role.

As indicated, the scope of coverage of the Commission covers virtually all of the data-collecting activity of the Government. It includes civil as well as criminal data.

The remainder of my remarks pertain to the assignment to the Federal Privacy Commission of criminal justice records and of law

enforcement records in their totality, barring none. The field of criminal justice records, I submit, is of such complexity that it should not be dealt with on the same terms as civil records. It should be the subject of separate regulation.

The field of criminal justice records and the related information, if it were not handled properly, would be dangerous to informants, operatives, agents, and officers of the law.

Mr. President, there is no need for this legislation to get into the regulation of criminal justice records. There is presently pending in Congress legislation—which now is narrowing down to its final stages—that deals specifically with criminal justice history, with criminal information centers, with data banks, court records, and all the other information which pertains to law enforcement.

This legislation, S. 2963 and S. 2964, is well along, and it is near resolution. It has been the subject of extensive hearings. Many hours have gone into perfecting its provisions.

It is a difficult field in itself and with its specific points—very difficult. Because of its complexity, the legislation has not been treated superficially and has, therefore, taken a period of time in which to reach the near-completion stage it now occupies.

With all this effort, in the passage of the pending bill, S. 2418, we would have superimposed upon the criminal-justice field very general rules which were designed for civil record systems and do not properly fit law enforcement. This would cause no end of confusion and no end of conflict.

Generally, it has been assumed that criminal justice or law enforcement information (whether used by Government or in the private sector) gives rise to problems requiring treatment different from that of information used to carry out social, health, or money benefit programs, to administer revenue and regulatory laws, to select and manage employees and outside contractors, and to conduct the multiplicity of other operations by Government or business. However, even within the broad range of separate informational relationships between individuals and Government or between individuals and business, where criminal detection and apprehension or enforcement of regulatory laws is not the object, wide differences occur. Material differences occur in the kinds and volume of information used, in the manner of collecting and disseminating information, in the degrees of data sensitivity, in the uses made of the information, and in the risks of possible abuse.

The Committee on the Judiciary is formulating this criminal justice data legislation, S. 2963 and S. 2964. The Judiciary Committees of the House and the Senate, have, through the years, acquired a great deal of experience and seasoning in this area. I submit that it is only fitting and proper, as well as wise, to reserve the responsibility of drafting complex legislation to those committees which developed background and expertise on the topic in question.

The job can be done, Mr. President, to protect privacy in the area of law enforcement records and criminal information centers. It can be done in a way to assure privacy and to assure relevance, to assure timeliness and completeness and accuracy of the data involved. That will be done. But it can be done best by those who are versed and knowledgeable in that field.

It is imperative that competent, seasoned, and expert authorities handle situations of that kind. The goal, after all, in law enforcement is good police work, good investigation work, good prosecution,

sentencing, and correction. Legislation should be enacted which considers these various aspects of law enforcement. In acting in this area we must insure that we have struck a proper and equitable balance between the individual's right to privacy and society's interest in good and effective law enforcement.

Mr. President, again I say that I do believe that the thrust of this bill, with its broad regulatory Commission and its effort to apply the same regulations to civil and criminal data—arrest records as well as intelligence information—is the wrong means to approach the problem with which we are attempting to deal. Happily, in the other body, there is being perfected a companion bill which has approached the matter in a vastly different way. It is my hope that in due time, rather than trying to amend this bill on the floor of the Senate, which would be a mighty poor way of trying to legislate in such a complex field, that we should make an effort to consider the product of the other body.

Again, I want to say that the objectives of S. 3418 are good. They are fine, and there will be a great deal of popular support for an attempt to correct practices which sometimes result in abuse of privacy. But it is not the label of the bill, it is not its declared programs for which we should vote; it is rather the fashion in which it is sought to achieve those objectives that really counts.

Mr. President, I yield the floor.

Mr. PERCY. Mr. President, I certainly think that the remarks of our distinguished colleague, Senator Hruska, are worthy of comment and the concerns he has raised are worthy of consideration. S. 3418 requires that criminal history and arrest records—that is, routine records of arrest and court decisions or rap sheets—be subject to the requirements of the bill.

But our bill does make a careful, proper distinction between this type of criminal record and another type. The latter type are criminal intelligence and investigative files.

These files, of course, are of a sensitive nature, and S. 3418, in section 203, provides that agencies maintaining such files may exempt them from the provisions of the bill providing that people may have access to their own records. We believe this exception to be proper and ample to meet the legitimate concerns of the law enforcement agencies.

The kinds of exception that arose, that have given such great emphasis to this bill, are the kind of situation which a mail cover picks up the fact that a high school girl—in this case, it was a girl by the name of Lori Paton—wrote a letter in connection with a high school theme to an agency that happened to be on the FBI's subversive list. The mail surveillance picked up that she was corresponding with such an agency, and she was therefore named in the record, and a high school girl had an FBI record.

All she was doing was writing a high school theme. She was not a subversive, but there she was, she had a file with the FBI. The family literally had to go to court and sue the Government in order to have that record taken out, along with all the other people that might be in such a position.

Our bill is so carefully drafted, that it would permit her to obtain access to her file. However, if the information in her file were in fact

criminal intelligence information, part of a current investigation of criminal activities, our bill would safeguard the ability of law enforcement personnel to withhold information until the possibility of prosecution had passed.

Certainly, we have no intention of interfering with criminal records and that type of thing, which the distinguished Senator pointed out must be preserved.

I think the bill has been carefully drawn in this regard. Nothing in S. 3418 would do damage to the quality of arrest records, for instance.

No excessive burdens for law enforcement agencies are created by this bill. Indeed, the specific legislation that the administration has sent to Congress to deal with criminal arrest records, and the two Senate bills—Ervin and Hruska—all of which are far more detailed and comprehensive in their treatment of arrest records, are not inconsistent with the treatment provided by S. 3418. All of these bills provide the same basic protections: an individual can see his own "rap sheet," the information must be accurate and up-to-date, and standards are established to regulate the disclosure and access to arrest record files.

S. 3418 provides these same minimum safeguards, to become effective 1 year after enactment. This delay allows time to permit a more explicit criminal records bill to be passed. However, until a bill passes there is no reason not to provide minimum standards.

The need for criminal records coverage is demonstrated by the NCIC—National Crime Information Center—a centralized national computer center that collects and disburses information about wanted persons, stolen property, and criminal history records, now operates without legal privacy restrictions. As of December 1, 1973, there were more than 5 million active files in this system. Computer terminals located in cities and towns all across the nation create easy access to these records. "They could lead to access by more users and for checking on more individuals than is socially desirable"—from the July 1973 HEW report on privacy. If harmful information about a person were placed in the file, it would be disseminated and available nationwide.

The HEW report says:

> In practice, the NCIC does not have effective control over the accuracy of all the information in its files. If a subscribing system enters a partially inaccurate record, or fails to submit additions or corrections to the NCIC files (e.g., the return of a stolen vehicle or the disposition of an arrest), there is not much that the NCIC can do about it.

Our bill would require the FBI, which administers the NCIC, to develop procedures to insure that information disseminated by NCIC is accurate, complete and up-to-date.

The HEW report continues to say that—

> Once a subscribing police department contributes an arrest report to the NCIC, that report is available to any "qualified requestor" in the system.
>
> In some states, this means employers and licensing agencies (for physicians, barbers, plumbers and the like). Thus, unless a criminal record information system is designed to keep track of all the ultimate users of each record released, and of every person who has seen it, any correction or emendation of the original record can never be certain to reach holder of a copy.

Our bill requires a complete log of all disclosures of personal information to individuals outside the agency maintaining the data.

Mr. HRUSKA. On that score, my main point pertains. To do something like that should be not through some board that has no expertise or exposure to that type of thing; the Congress, through its oversight powers over the FBI and the Department of Justice and so on, would be able to take care of that. The proposed legislation, S. 2963 and S. 2964 does, and if it is in the field of security, or if it is in the field of something else, the proper legislative body, oversight body, can deal with that very satisfactorily, without getting into this nebulous and innovative area and something really new that would be loosed upon the width and breadth of the land.

Mr. ERVIN. Mr. President, I wish to reply very briefly to the distinguished Senator from Nebraska (Mr. Hruska).

This bill does not empower the Privacy Commission to have any jurisdiction over any other agency of Government except to the extent that that other agency of Government is engaged in collecting or storing or disseminating personal information about individuals. Outside of that, it has no jurisdiction whatever.

The term, "personal information" is defined in subsection 2 of section 301 of the bill, on page 48.

The bill is a very simple bill when you stop to analyze it sufficiently. In the first place, it says that Government shall not call on individuals for any information unless that information is reasonable or necessary to enable the agency asking for it to perform its statutory duties. Then it requires Federal agencies to restrict that information—that is, personal information only. They will restrict its disclosure to officials who have some public duty to perform that requires them to have access to that information.

Then it provides that no information will be released to unauthorized persons.

Those are very simple requirements.

With reference to law enforcement provisions, it expressly provides that the head of any law enforcement agency can exempt the agency from certain crucial provisions of the bill. It will not impede the agency's operations as a law enforcement agency.

With reference to the CIA, the Senate has adopted an amendment today, among other amendments, which virtually relieves the CIA from coverage by the act, except to the extent that it must file some reports.

This is a very simple bill, with simple features. It is necessary to give the Privacy Commission some power to enforce it; otherwise, it will be just a hollow piece of legislative mockery on the statute books. I sincerely hope that the Senate will pass it.

AMENDMENT NO. 1992

Mr. WEICKER. Mr. President, I call up my amendment No. 1992, and ask for its immediate consideration.

The legislative clerk proceeded to read the amendment.

Mr. WEICKER. I ask unanimous consent that further reading of the amendment be waived, and that the amendment be printed in the Record.

The PRESIDING OFFICER (Mr. Pearson). Without objection, it is so ordered.

Mr. Weicker's amendment (No. 1992) is as follows:

On page 54, line 8, strike out "This Act" and insert in lieu thereof "Titles I, II, and III of this Act".

On page 54, line 14, strike out "this Act" and insert in lieu thereof "titles I, II, and III of this Act".

On page 54, immediately below line 14, insert the following new title:

"TITLE IV—FINANCIAL DISCLOSURE

"SEC. 401. This title may be cited as the 'Net Worth Disclosure Act'.

"SEC. 402. (a) Each individual referred to in subsection (b) shall file annually with the Comptroller General of the United States a full and complete statement of net worth to consist of:

"(1) A list of the identity and value of each asset held by him, or jointly by him and his spouse or by him and his child or children, and which has a fair market value in excess of $1,500 as of the end of the calendar year prior to that in which he is required to file a report under this Act.

"(2) A list of the identity and amount of each liability owed by him, or jointly by him and his spouse or by him and his child or children, and which is in excess of $1,500 as of the end of the calendar year prior to that in which he is required to file a report under this Act.

"(b) The provisions of this Act apply to the President, the Vice President, each Member of the Senate, each Member of the House of Representatives (including Delegates and the Resident Commissioner from Puerto Rico), and each officer and employee of the United States within the executive and legislative branches of Government receiving compensation at an annual rate in excess of $30,000.

"(c) Reports required by this Act shall be in such form and shall contain such information in order to meet the provisions of this Act as the Comptroller General may prescribe. All reports filed under this Act shall be maintained by the Comptroller General as public records, open to inspection by members of the public, and copies of such records shall be furnished upon request at a reasonable fee.

"SEC. 403. Each person to whom this Act applies on January 1 of any year shall file the report required by this on or before February 15 of that year. Each person to whom this Act first applies during a year after January 1 of that year shall file the report required by this Act on or before the forty-fifth day after this Act first applies to him during that year.

"SEC. 404. Any person who knowingly and willfully fails to file a report required to be filed under this Act, or who knowingly and willfully files a false report required to be filed under this Act, shall be fined not more than $2,000, or imprisoned for not more than two years, or both.

"SEC. 405. This title shall become effective on January 1, 1975.".

Mr. WEICKER. Mr. President, to digress briefly, I do not know how many more occasions I will have to speak of my admiration for the distinguished Senator from North Carolina, an admiration that has grown during my years here in the Senate, as I have seen him devote his energies to a piece of paper that, very frankly, has almost been forgotten, specifically, the Constitution of the United States.

You know, there is no greatness in this land that does not spring from that document. That which is good, tangibly good, that we see around us, is the manifestation of its great concepts and its great ideals. At a time when so many people had forgotten those concepts and ideals, it was the Senator from North Carolina who gave them legislative meaning and, indeed, very practical meaning, to the people of this country.

So, regardless of our respective positions on any amendments that I have to offer to this bill, the fact is that I want to express now my humble admiration for Senator Ervin's great contribution to this Nation, at a time when such was very specifically called for. He was the only one, at a certain time, to stand up and be counted.

I am today offering an amendment to the Federal Privacy Board Act to require the full disclosure of net worth by high-ranking officials in the executive and congressional branches of Government. This amendment is the same as the net worth disclosure bill, S. 4059, which I originally introduced before the Senate on September 30.

I ask unanimous consent that the name of the distinguished Senator from Oklahom (Mr. Bartlett) be added as a cosponsor of the amendment.

The Presiding Officer. Without objection, it is so ordered.

Mr. Weicker. It is a matter of particular concern to me that the Congress has not yet enacted legislation to guarantee to the public the right to know the financial interests of those who guide their Government. I strongly believe that the public has that right and that the disclosure of financial worth by policymakers is one step toward strengthening the public trust in Government.

Obviously, we consider this matter of the financial interests of public officials to be of importance, otherwise we would not be spending the time spent already in making such inquiries of a potential Vice President of the United States. There is not one single confirmation hearing that we conduct in the Senate that does not have as a key part of the hearing a statement of assets and liabilities and the elimination of any assets and liabilities which we demand, where any conflict of interest might arise.

During floor consideration of the Federal Election Campaign Act, I supported and the Senate passed an amendment that would have required public reporting by elected Federal officials of personal financial affairs. This amendment would have covered each candidate for election to Congress, Members of Congress, the President, the Vice President and certain U.S. officers and employees, at GS–16 level or earning more than $25,000 per year.

Reports of financial interests would have been filed with the Federal Election Commission and would have included:

First, amounts of Federal, State, and local income or property taxes paid:

Second, amount and source of each item of income or gift over $100;

Third, identity of assets and liabilities over $1,000;

Fourth, all dealing in securities and commodities over $1,000; and

Fifth, all purchases or sales of interest in real property involving over $1,000, except for personal residence.

However, this amendment, passed in the Senate by voice vote, was deleted afterwards during conference consideration of the Federal Election Campaign Act. The Federal Election Campaign Act, as passed into law, contained no provision for financial disclosure—public financial disclosure—by elected and appointed Federal officials.

The amendment that I am proposing today is simple and straightforward. It is not as comprehensive as the previous disclosure amendment that was deleted in conference—but seeks to establish in law minimal disclosure requirements for elected Federal officials.

Those covered by the act would be the President, the Vice President, Members of the Senate, Members of the House of Representatives, and all employees of the executive and legislative branches receiving compensation at an annual rate of more than $30,000.

What and when do they have to file? Annually with the Comptroller General a list of all assets and liabilities over $1,500, on the basis of fair market value as of December 31 of the previous year. All reports filed with the Comptroller General are to be maintained by the Comptroller General as public records, open to inspection by members of the public.

The act would become effective as of January 1975. The time period covered would be the preceding calendar year. Therefore, by February 15 of 1975, all persons covered by this legislation would have to indicate what their net worth was as of December 31, 1974. Anyone who had been appointed or elected in a public election during the course of 1975 would have to file such a statement within 45 days of his election or appointment.

I recognize that the bill we are dealing with concerns privacy, a need for which, as I have already indicated, has always been of deep concern to the distinguished Senator from North Carolina. Indeed, the distinguished Senator from Illinois has also been a leader in assuring this most basic right.

I predict right now that the question of the right to privacy will be one of the great issues of the 1970's and 1980's. It goes to the very basis of the Constitution which the Senator from North Carolina has so ably defended over the years.

I think it is important to point out on every occasion that we can that the difference between our political system and that of any other nation in today's world, or indeed throughout history, is that our Constitution and our political system focus on the individual, not on society as a whole—not on the mass, but on the individual.

If we want something that is efficient, trouble free, and expeditious, it cannot be the Constitution of the United States. How can we have something that is quiet, efficient, and trouble free when it concerns itself with 210 million people? It is impossible. That is why the issue of privacy is important—so that we preserve that spirit which has guaranteed to each human being in this country a full flowering of their abilities and their aspirations and their hopes. That opportunity for individual flowering has given us a magnificent historical experience.

So this is not an academic issue, to be debated by scholars and professors, but indeed it goes to the very heart of our experience as a nation.

Mr. President, just to wrap up my comments relative to this amendment, there are those areas, however, where I think that what we do not want is privacy and secrecy. We want openness; we want sunshine. Specifically, I speak of that which deals with those in positions of public trust.

I find it rather ironic that we have recently sat through a number of well-publicized Senate hearings and still do not impose upon ourselves the same requirements we have been imposing upon those being investigated. If we want credibility in this country, indeed, what is sauce for the goose is sauce for the gander. I think quite properly this must be so in this country, so that people might understand our actions in relation to our economic interests.

This is the reason that, despite my desire to guarantee the privacy of individuals, I want our lives as elected officials to be totally open to scrutiny by the American people.

I propose to achieve such an end by virtue of this amendment which is very, very simple, a listing of those assets and liabilities over $1,500 once a year by every one of us, by the President, the Vice President, his Cabinet officers, those highly paid staff members, which documentation would be available to the public upon request.

I would hope, Mr. President, that my colleagues would see fit to impose this obligation on themselves, and I think it would do a great deal to bring us up the ladder of respect in the eyes of the American people.

I might add that I believe most of the individuals whom I see in this Chamber have done that anyway. I am not pointing any finger, but I would just like to see us go ahead and make it a matter of law rather than a matter of individual discretion.

Mr. ERVIN. Mr. President, as I observed earlier, if we take on legislative nag and put too heavy a load on it, the nag might not be able to reach its intended destination.

Ever since I have been in the Senate there have been amendments proposed from time to time on the floor with reference to disclosure of the assets of Senators.

I have never known, however, of any committee to conduct any hearing on any bill of that kind, and I think it is a matter that ought to be explored by the appropriate committee, or there ought to be a hearing, or there ought to be a decision based on a hearing on this subject.

I respectfully submit that this amendment is not really germane to this bill. This bill is a bill to regulate how the agencies of the Federal Government shall conduct themselves in respect to the collection, the storage, the use and the dissemination of personal information, and I hope that the Senator from Connecticut will not press his amendment for that reason.

I do not want to jeopardize this bill. I think we have got a good bill here.

I am going to introduce in a few days a bill encompassing some of the election reforms recommended by the Senate Select Committee on Presidential Campaign Activities which have not been enacted into law, and I think the Senator's amendment would be quite appropriate for consideration in connection with that legislation.

I will cease to be chairman of the Government Operations Committee on the expiration of my present term in the Senate. I trust, according to all the precedents, that my colleague, the distinguished Senator from Connecticut (Mr. Ribicoff), will be my successor. I hope that he can give the Senator assurance that it would be considered, either in the introduction of legislation to implement the recommendations of the Senate select committee or as an independent bill.

I hope that the Senator from Connecticut (Mr. Weicker) will not press his amendment because it might jeopardize this particular bill which is restricted in its nature to Government action rather than action of individuals.

I want to thank the distinguished Senator from Connecticut (Mr. Weicker) for his most gracious and generous remarks that he made concerning my activities as a Member of the Senate.

Ever since he came to the Senate, he has had offices across the hall from my offices, and I have had very many contacts with him.

I do not know any Senator who has ever rendered more intelligent and more courageous service in any particular field than the Senator

from Connecticut (Mr. Weicker) rendered to this country and to this Senate as a member of the Senate select committee. I cannot pay him too high a tribute for his intelligent and courageous actions in that respect.

Mr. WEICKER. I thank the Senator.

Mr. RIBICOFF. I have been apprised of the colloquy between the Senator from North Carolina, the chairman of the Government Operations Committee, and my esteemed colleague from Connecticut, Senator Weicker.

First, I can only make assurances, subject to the Senate naming me to succeed our esteemed chairman, Mr. Ervin, chairman of the Government Operations Committee.

But should I be designated as chairman of the Government Operations Committee when we meet in session next year, I assure my colleague from Connecticut that in connection with the hearings on the Ervin bill, which is an outgrowth of the important reforms suggested by the Select Committee on Presidential Campaign Activities, I would also believe it appropriate to have hearings on the proposal of my colleague from the State of Connecticut.

I would assure him that, in conjunction with the hearings on the Ervin bill, we could proceed with hearings on the Weicker bill and adopt it, if the committee so agrees, Mr. Weicker.

Mr. WEICKER. I thank my colleague.

Mr. BAYH. Mr. President, will the Senator from Connecticut (Mr. Weicker) yield to the Senator from Indiana?

Mr. WEICKER. Yes.

Mr. BAYH. I listened with a great deal of interest to what I thought was a very eloquent, appropriate, and on-the-mark assessment of the validity behind the amendment of my distinguished friend and colleague, the Senator from Connecticut.

This is very much along the same lines of a measure introduced by the Senator from Indiana some time ago, and I would like to suggest to my other distinguished colleague, the Senator from Connecticut, that if we are exploring that situation next year, which I certainly hope we will, we look at the need to broaden disclosure beyond the current boundary lines as well as examining our measure suggested by our distinguished colleague from Connecticut.

As the Senate may recall, we had a very difficult battle on this floor relative to the merits of a certain Supreme Court judge. One of the significant aspects of that debate, and one of the issues which I feel we did not agree upon, was a conflict of interest that concerned many of us and led to his not being confirmed by the Senate.

At that time, it seemed to me that we should deal with judicial conflicts of interests as well as in the legislative and executive branches.

So I would suggest that in looking into this, we include the importance of disclosure with regard to judicial conflicts of interest, as to their propriety or appearance of propriety, and that we also explore lowering that dollar figure down to $1,800. We have a number of people on our staffs and in executive positions who are making decisions behind closed doors, away from public assessment and disclosure to our constituents generally, who have, perhaps, as much influence in making decisions as some of the rest of us who are in the limelight all the time.

So I want to compliment my distinguished colleague, the Senator from Connecticut, and I would like to join with him and ask him to join with me in studying this.

I also hope that my other friend and colleague, the Senator from Connecticut, who has been here now for 12 long years with the Senator from Indiana, will start the 13th by exploring the very important aspects of putting it all on top of the table and letting our constituents then judge whether this really is a conflict of interest.

Mr. RIBICOFF. May I respond to my distinguished colleague from Indiana that should such a proposal be included in the bill to be presented by the Senator from Connecticut or by the Senator from Indiana, and it is referred to the Government Operations Committee, we could certainly explore through hearings the proposal of the Senator from Indiana at the same time. I would certainly so assure the Senator from Indiana.

Mr. WEICKER. Mr. President, I certainly accept the assurances of my distinguished colleague from Connecticut and the Senator from North Carolina.

Mr. PERCY. And the Senator from Illinois, as ranking minority member, would like to join in assuring the Senator from Connecticut that hearing will be held.

Mr. WEICKER. Mr. President, under those circumstances, admittedly it is certainly less than germane. You see, the last time the amendment was offered it was on a bill which it was said was not germane either, so I thought we might try something that was less than germane to have it become law.

I know that we will have hearings and believe me, it would certainly enhance the image of this body. The eyes of the American people should be addressed to this separate subject, and legislation should be enacted right away. With those remarks, I ask that the amendment which I have offered be withdrawn.

The PRESIDING OFFICER (Mr. Helms). The Senator has the right to withdraw his amendment.

Mr. ERVIN. Mr. President, I ask for the yeas and the nays on final passage.

The PRESIDING OFFICER. Is there a sufficient second?

The yeas and the nays were ordered.

Mr. WEICKER. Mr. President, I send an amendment to the desk.

The PRESIDING OFFICER. The clerk will report the amendment.

The second assistant legislative clerk read as follows:

On page 43, line 2, strike the (;) and insert the following:

", provided such personal information is transferred or disseminated in a form not individually identifiable."

On page 47, line 23, strike the (-) and insert the following:

", provided such personal information is transferred or disseminated in a form not individually identifiable."

Mr. ERVIN. Mr. President, the amendment referred to by the Senator from Connecticut is meritorious and I hope the Senate will adopt it.

Mr. WEICKER. I thank the Senator from North Carolina. What this does is attack the confidentiality of our income tax returns. It is as simple as that. With my amendment—the relevant information is available. However, as far as the individual return and identity of the

return is concerned, no, it is not available to the Census Bureau, and should not be. I am delighted my amendment is acceptable to the Senator from North Carolina.

I hope we can get the point home to the people downtown. I file my tax return for the purposes of collection of taxes and nothing else.

This amendment does that. The generalized information is available, but not the specific return.

The PRESIDING OFFICER. The question is on agreeing to the amendment of the Senator from Connecticut.

The amendment was agreed to.

The PRESIDING OFFICER. The bill is open to further amendment.

Mr. BAYH. Mr. President, a parliamentary inquiry.

The PRESIDING OFFICER. The Senator will state it.

Mr. BAYH. Mr. President, we are not operating under controlled time?

The PRESIDING OFFICER. That is correct.

Mr. BAYH. Mr. President, I would like to add my word of commendation to the distinguished Senator from North Carolina for the significant contribution he has made as represented here in this bill.

I would like to go further, if I might, as one who has had the good fortune of sitting with him as a member of the Constitutional Rights Subcommittee for a number of years, to suggest that the product of this bill is like one acorn in the forest compared to the hours of work contributed by our distinguished friend from North Carolina.

My friend from North Carolina and I have not always agreed on issues that have been before this body, but I must say it has been like a breath of fresh air for some of us who believe that the first 10 amendments of the Constitution are as absolutely indispensable today as when they were introduced long ago, to see a champion like the distinguished Senator from North Carolina stand up and lead the charge in defending these rights from attack.

I must say, I have a lump in my throat, if I might say it as unemotionally as I know how, to think of the void that will exist when he leaves the Congress.

I suppose most of us here are dedicated to the principles of the Bill of Rights, but I know of no other person who has had a greater feel for the indispensability of these amendments and a willingness to put the work and the effort behind that dedication. I just cannot thank him enough.

He has been more prominently on the national scene as a result of his work in the Watergate hearings, and we owe him a debt for that, but I think perhaps an even greater debt goes to the effort he has been leading a long time before anybody heard of Watergate.

I think if this Nation and this body had listened to what the Senator from North Carolina was trying to say over the years, and certainly if the Department of Justice and some of those folks who succumbed to temptation down at the White House had listened to what he was trying to say, there would never have been a Watergate.

Now, may I ask my distinguished colleague from North Carolina if he would care to give us his opinion, for the record, relative to the importance of the Committee on the Judiciary continuing to explore any violations of our individual rights, privacy, and the area of personal information systems and data banks?

I note this is a joint effort of governmental operations and the Judiciary Subcommittee of which he was chairman.

I would not, by default, want the Judiciary Committee, which he served so faithfully through the years and which was moving in this area, to lose jurisdiction or the opportunity to continue the vigilance he established at quite a high level.

Mr. ERVIN. Mr. President, first I want to thank my good friend from Indiana for his most generous and gracious remarks.

I also want to say that while he and I have differed at times on certain issues, that we have never disagreed about the value of the Bill of Rights as a guarantee of the freedom of all Americans.

On all occasions when I have been fighting for the Bill of Rights, he has been by my side.

The Government Operations Committee had jurisdiction of this particular bill because it does affect the structure of the Government in that it creates a Federal Privacy Board.

I recognize also in the sense that the Judiciary Committee, through its Subcommittee on Constitutional Rights, had a concrete jurisdiction because this involves some of the basic constitutional rights of Americans.

I do not think passage of this bill will alter in any way the provisions of the rules which give the Subcommittee on Constitutional Rights as part of the Judiciary Committee jurisdiction to investigate and initiate legislation dealing with constitutional rights in the field of privacy or any other field where they exist.

Mr. BAYH. I appreciate the Senator's assessment in this area.

Might I also ask him to give us the benefit of his thoughts or feeling in some additional areas. I understand there are restrictions between what we might like to accomplish and what we feel we have 51 votes for. One of the concerns that the Senator from Indiana had addressed in other legislation is the existence of other kinds of information-gathering systems that are now under the jurisdiction of State or local governments, or indeed in the private sector with particular concern expressed about the credit rating business. Could the Senator give us his thoughts on this?

Mr. ERVIN. Well, the Government Operations Committee and the Subcommittee on Constitutional Rights agreed to restrict the provisions of this bill very narrowly and to make it apply primarily to the information-gathering activities affecting an individual on the part of the Federal agencies.

We originally did have provision to apply it to the States, but there was some considerable opposition to it. As a pragmatic matter we restricted coverage of the bill, as far as States are concerned, to a study of State agencies. The provisions of the bill do apply to a State agency which is created by a grant or contract with the Federal agency where it sets up a computer system. Otherwise, it does not apply to States.

We also restricted its application insofar as individuals' private affairs are concerned for the pragmatic reason we felt that if we tried to deal with the whole subject in one bill, we would be inviting considerable opposition.

I agree with the Senator from Indiana that it is a very serious question which arises as to the privacy of Americans by the activities of

credit corporations and that there should be some legislation in the Federal field to safeguard the individual's right of privacy in respect to such credit organizations and similar organizations engaged in commercial business.

Mr. BAYH. I certainly appreciate the Senator's thoughts on this. Might I ask him to give his attention to one other area?

I am quite concerned about the exemption clause in section 203, subsections (a) and (b). I am concerned because whenever you set up an exemption, the question is how broad is the exemption.

As the Senator from Indiana reads this, we are talking specifically about national defense and foreign policy, and intelligence and investigation information.

Does the Senator suggest that this should be narrowly defined, particularly when we look at foreign policy? It is a rather broad construction that could be interpreted from this exemption.

Mr. ERVIN. I think that "national security" embraces foreign policy in a sense. There is an executive order which says that national security embraces only two things: our national defense, that is, our defense posture, our armed services and plans in that connection; and our sensitive dealings with foreign countries.

I think that the first one of these exemptions would include those things.

While the bill does allow the head of an agency engaged in investigatory work for criminal law enforcement purposes to exempt the agency if he finds the provisions regulating the dissemination of these records, and so on, of individuals would impede the accomplishment of his department's professional duties or statutory duties.

I think those are narrow restrictions. I think they are essential if we are going to get a bill that will command the majority of both Houses of Congress, and one that will be signed into law by the President. We have to take those practical considerations into effect.

Also, I would doubt the advisability of Congress' creating a new agency and giving it some jurisdiction to veto the action of long-established law enforcement agencies.

Mr. BAYH. My concern, as I am sure the Senator from North Carolina understands, is based on the fact that it is some of those agencies that have been the primary culprits in violating these rights which he cherishes and has done so much to protect in the past.

Mr. ERVIN. Yes. Of course, that is one trouble: whenever power is lodged, it is always subject to be abused. But you have to lodge power somewhere in order to get things done.

Mr. BAYH. In talking about national defense and foreign policy, and in talking about intelligence and investigative information, is it the Senator's assessment that we are talking about three agency heads there, or three general departments?

Mr. ERVIN. The FBI, in the first place. Also, the Secret Service. Also, the Customs people who have certain law enforcement powers. Generally, you would have the CIA also.

However, we offered an amendment which was adopted and which only requires the CIA to make reports to the Commission with respect to its intallations and does not require them to divulge information. When they stay within their field, as they apparently did not do in

the case of Chile, they are concerned solely with national security in foreign areas.

Mr. BAYH. I assume we are also talking about the Secretary of Defense? And the Secretary of State, perhaps?

Mr. ERVIN. Yes, to a limited degree, where he is engaged in enforcing military law.

Mr. BAYH. What concerns me is that it could not be a reasonable interpretation that, for example, the Secretary of Agriculture or somebody dealing with Public Law 480 which affects our foreign policy, or the Secretary of Commerce, which, in some instances, would also be affecting our foreign policy, to be able to utilize these two exemptions as a way to get themselves out from under the restrictions of this legislation.

Mr. ERVIN. I do not think it would bother anybody except those engaged in investigative work either to protect national security or the enforcement of the criminal laws. That is not the function of the Department of Agriculture.

Mr. BAYH. I share that belief, but I think it makes a lot more sense and makes better legislative history coming from my distinguished friend from North Carolina.

One last question: In subsection (c) on page 45, where we talk about a determination to exempt any such system, and go on and talk about the head of any such agency on line 23, are we talking specifically and only about those agencies covered in subsections (a) and (b)?

Mr. ERVIN. That is right.

The word "such" there is just like we lawyers so frequently say the said agencies or aforesaid agencies specified in those two preceding sections.

Mr. BAYH. I appreciate the patience of my good friend as well as his great contribution.

Mr. ERVIN. Thank you very much.

AMENDMENT BY SENATOR BIDEN

Mr. BIDEN. Mr. President, I send an amendment to the desk and ask for its immediate consideration. I understand that both the majority and minority members have agreed to this amendment.

The PRESIDING OFFICER. The amendment will be stated.

The legislative clerk read as follows:

On page 22, line 17, insert the following new section:

"h(1) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress.

(2) Whenever the Commission submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress."

Mr. BIDEN. Mr. President, the amendment I have offered would help to insure that the Privacy Protection Commission which would be established by this bill. Would truly be an independent regulatory

agency. The amendment would require that the Commission submit to Congress a copy of virtually every communication it has with the President or the Office of Management and Budget in regard to budgetary or policy matters.

Furthermore, when the Commission offered legislative recommendations to Congress, neither the President, the Office of Management and Budget nor any other Federal agency or officer—could require that the Commission clear its remarks with them first.

Mr. President, as events of the last 2 years have indicated, we can ill-afford to allow the executive branch to control our supposedly independent agencies.

These agencies are instruments not only of the executive, but also of the Congress. This amendment will allow Congress to act as a watchdog to determine that it receives the agencys' views as to policy and budget, not the executive's. In other words, we will be able to determine for ourselves not only the needs of the Commisison, but its advice and its problems.

Furthermore, by playing this watchdog role, perhaps we can curtail the common practice of an agency submitting an overly large budget knowing full well that the Office of Management and Budget would cut it.

This amendment would not only allow us to scrutinize the actions of the Executive regard to the Commission, but to also scrutinize the actions of the Commission itself.

In 1972, an identical provision was enacted as part of the legislation creating the Consumer Product Safety Commission. The provision has apparently proved to be very effective. For the first time, discussions between the budget office and a regulatory agency have been transmitted to Congress. Since we must vote on the appropriations for such agencies, it seems only natural that we be able to see budget estimates from the agencies themselves, not after they have been sifted through the executive branch.

Mr. President, in this Congress we have taken great strides toward reasserting our control over such things as the budget. We have attempted to assure that the three branches of Government are truly coequal. My amendment to this bill would be one more step in that direction.

Mr. ERVIN. Mr. President, as I understand, this amendment merely requires the Privacy Board to be created by this legislation to file with the Congress its budget at the same time it files its budget request with the President. I think it is a wholesome, meritorious amendment. I hope the Senate will adopt it.

Mr. BIDEN. Everybody has been complimentary to the Senator from North Carolina. I would like to add my compliments, though I have not shared any lengthy amount of time with him in the Senate.

I compliment him on one thing that has been in short supply here—consistency.

I yield the floor.

The PRESIDING OFFICER. The question is on agreeing to the amendment of the Senator from Delaware.

The amendment was agreed to.

The PRESIDING OFFICER. The bill is open to further amendment.

Mr. ERVIN. Mr. President, I would like to ask to be printed in the Record at this point the marked portions of the committee report as marked by me from page 4 through page 14, which shows why we need this legislation.

The PRESIDING OFFICER. Without objection, it is so ordered.

There being no objection, the excerpt was ordered to be printed in the Record, as follows:

COMMITTEE OVERSIGHT

These hearings continued the oversight by the Government Operations Committee of the development and proper management of automated data processing in the Federal Government and its concern for the effect of Federal-State relations of national and intergovernmetal data systems involving electronic and manual transmissions, sharing, and distribution of personal information about citizens.

Senator Ervin announced the joint hearings as Chairman of both subcommittees, in a Senate speech on June 11 in which he summarized the issues and described some of the complaints from citizens which have been received by Members of Congress, as follows:

"It is a rare person who has escaped the quest of modern government for information. Complaints which have come to the Constitutional Rights Subcommittee and to Congress over the course of several administrations show that this is a bipartisan issue which effects people in all walks of life. The complaints have shown that despite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information-gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy make it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.

"The complaints show that many Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its powers to investigate and store information.

"They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it.

"They are concerned about intrusive statistical questionnaires backed by the sanctions of criminal law or the threat of it because they have been subject to these practices over a numbers of years."

S. 3418 provides an "Information Bill of Rights" for citizens and a "Code of Fair Information Practices" for departments and agencies of the executive branch.

Testimony and statements were received from Members of Congress who have sponsored legislation and conducted investigations into complaints from citizens; from Federal, State, and local officials including representatives of the Administration and certain departments and agencies, the Domestic Council Committee on Right to Privacy, the Commerce Department, Bureau of the Census, National Bureau of Standards, the General Services Administration, the Office of Telecommunications Policy; the National Governors Conference, the National Legislative Conference, the National Association for State Information Systems, and the Government Management Information Sciences. Many interested organizations and individuals with expert knowledge of the subject advised the Committee. These included the former Secretary of Health, Education, and Welfare, Eliot Richardson, authors of major studies, experts in computer technology, constitutional law, and public administration, the American Civil Liberties Union, Liberty Lobby, the National Committee for Citizens in Education, the American Society of Newspaper Editors, and others.

The provisions of the bill as reported, reflect the bill as introduced, with revisions based on testimony of witnesses at hearings, consultations with experts in privacy, computer technology, and law, representatives of Federal agencies and of many private organizations and businesses, as well as the staffs of a number of congressional committees engaged in investigations related to privacy and governmental information systems.

The Committee finds that the need for enactment of these provisions is supported by the investigations and recommendations of numerous congressional committees, reports of bar associations, and other organizations, and conclusions of governmental study commissions.

To cite only a few, there are:

Earlier studies of computers and information technology by the Senate Committee on Government Operations and the current hearings and studies relating to S. 3418;

The hearings and studies on computers, data banks and the bill of rights and other investigations of privacy violations before the Constitutional Rights Subcommittee;

The hearings and studies of computer privacy and government information-gathering before the Judiciary Administrative Practices Subcommittee;

The hearings on insurance industries and other data banks before the Judiciary Antitrust Subcommittee;

The hearings on abuses in the credit reporting industries and on protection of bank records before the Senate Banking, Housing and Urban Affairs Committee;

Investigations over many years by the House Government Operations Committee; and

Finally, there are many revelations during the hearings before the Select Committee on Watergate of improper access, transfer and disclosure of personal files and of unconstitutional, illegal or improper investigation of and collection of personal information on individuals.

Particularly supportive of the principles and purposes of S. 3418 are the following reports sponsored by Government agencies:

1. "Legal Aspects of Computerized Information Systems" by the Committee on Scientific and Technical Information, Federal Council of Science and Technology, 1972.

2. "Records, Computers and the Rights of Citizens", Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education, and Welfare, July 1973.

3. "Databanks in a Free Society, Computers, Record-Keeping and Privacy", of the Computer Science and Engineering Board, National Academy of Sciences, by Alan F. Westin and Michael Baker.

4. Technical Reports by Project Search Law Enforcement Assistance Administration, Department of Justice.

5. A draft study by the Administrative Conference of the United States on Interagency Transfers of Information.

6. Report by the National Governors Conference.

7. Reports by international study bodies.

The ad hoc subcommittee has initiated two surveys of the Governors and of the attorneys general of the States which are producing responses supportive of congressional legislation on privacy and Federal computers and information technology. They also reveal strong efforts in State and local governments to enact similar or stronger legislation to protect privacy.

The need for the bill is also evident from the sample of legal literature and public administration articles and press articles reprinted in the appendix of the subcommittee hearings.

Finally, there are the complaints of information abuses received by many Members of Congress and diligently investigated by each of them.

Dr. Alan F. Westin, director of the 1972 National Academy of Sciences Project, reported that the study suggested "six major areas of priority for public action: laws to give individuals a right of notice, access, and challenge to virtually every file held by local, State, and national government, and most private record systems as well; promulgation of clearer rules for data-sharing and data-restriction than we now have in most important personal data files; rules to limit the collection of unnecessary and overbroad personal data by any organization; increased work by the computer industry and professionals on security measures to make it possible for organizations to keep their promises of confidentiality; limitations on the current, unregulated use of the Social Security number; and the development of independent, 'information-trust' agencies to hold especially sensitive personal data, rather than allowing these data to be held automatically by existing agencies."

Witnesses cited the failure of legislation and judicial decisions to keep pace with the growing efficiency of data usage by promulgating clear standards for

data collection, data exchange, and individual access rights. Similarly, many other witnesses before Congress agreed with his judgment that the mid-1970's is precisely the moment when such standards need to be defined and installed if the managers of large data systems, and the specialists of the computer industry, are to have the necessary policy guidelines around which to engineer the new data systems that are being designed and implemented.

Dr. Westin cautioned:

"To delay congressional action in 1974–75, therefore, is to assure that a large number of major data systems will be built, and other existing computerized systems expanded, in ways that will make it extremely costly to alter the software, change the file structures, or reorganize the data flows to respond to national standards. And beyond the money, such late changes threaten to jeopardize many operations in vital public services that will be increasingly based on computerized systems—national health insurance, family assistance plans, national criminal-offender records, and many others. In fact, these systems may become so large, so expensive, and so vial to so many Americans that public opinion will be put to a terrible choice—serious interruption of services *or* installation of citizen-rights measures."

The spread of the data bank concept, the increasing computerization of sensitive subject areas relating to people's personal lives and activities, and the tendency of government to put information technology to uses detrimental to individual privacy were detailed by Professor Arthur Miller. He stated:

"Americans today are scrutinized, measured, watched, counted, and interrogated by more governmental agencies, law enforcement officials, social scientists and poll takers than at any other time in our history. Probably in no Nation on earth is as much individualized information collected, recorded and disseminated as in the United States.

"The information gathering and surveillance activities of the Federal Government have expanded to such an extent that they are becoming a threat to several of every American's basic rights, the rights of privacy, speech, assembly, association, and petition of the Government.

* * * * * * *

"I think if one reads Orwell and Huxley carefully, one realizes that "1984" is a state of mind. In the past, dictatorships always have come with hobnailed boots and tanks and machineguns, but a dictatorship of dossiers, a dictatorship of data banks can be just as oppressive, just as chilling and just as debilitating on our constitutional protections. I think it is this fear that presents the greatest challenge to Congress right now."

Professor Miller characterized the reported bill as "a major step in developing a rationale regulatory scheme for achieving an effective balance between a citizen and the Government in the important field of information privacy. The creation of a Privacy Protection Commission with broad power of investigation, reporting, and suasion seems to me to be an effective way of developing policy in this rapidly changing environment. Also worthy of enthusiastic support is Title II of the proposed legislation. We simply cannot allow more time to pass without developing standards of care with regard to the gathering and handling of personal information. In that regard, S. 3418 goes a long way to establish the much needed information bill of rights."

The four-year survey by the Constitutional Rights Subcommittee, intended as an aid to Congress in evaluating pending legislation, demonstrates the need for requiring the following Congressional action:

Explicit statutory authority for the creation of each data bank, as well as prior examination and legislative approval of all decisions to computerize files;

Privacy safeguards built into the increasingly computerized government files as they are developed, rather than merely attempting to supplement existing systems with privacy protections;

Notification of subjects that personal information about them is stored in a Federal data bank and provision of realistic opportunities to review and correct their own records;

Constraints on interagency exchange of personal data about individuals and the creation of interagency data bank cooperatives;

The implementation of strict security precautions to protect the data banks and the information they contain from unauthorized or illegal access; and

Continued legislative control over the purposes, contents and uses of government data systems.

HEW REPORT

Another report reflecting major provisions of S. 3418 is that rendered by the Secretary's Advisory Committee on Automated Personal Data Systems to the Department of Health, Education and Welfare. Former Secretary Elliot Richardson described their findings in his testimony.

The report found that "concern about computer-based record keeping usually centers on its implications for personal privacy, and understandably so if privacy is considered to entail control by an individual over the uses made of information about him. In many circumstances in modern life, an individual must either surrender some of that control or forego the services that an organization provides. Although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms."

"Under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices." For this reason, as well as because of the need to establish standards of record-keeping practice appropriate to the computer age, the report recommends the enactment of a Federal "Code of Fair Information Practice" for all automated personal data systems. The Code rests on five basic principles that would be given legal effect as "safeguard requirements" for automated personal data systems.

There must be no personal data record-keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for an individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[1]

The Advisory Committee recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems as follows:

The Code should define "fair information practice" as adherence to specified safeguard requirements.

The Code should prohibit violation of any safeguard requirement as an "unfair information practice."

The Code should provide that an unfair information practice be subject to both civil and criminal penalties.

The Code should provide for injunctions to prevent violation of any safeguard requirement.

The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits."

Pending the enactment of a code of fair information practice, the Advisory Committee also recommended that all Federal agencies apply these requirements to all Federal systems, and assure through formal rulemaking that they are applied to all other systems within reach of the Federal government's authority. Beyond the Federal Government, they urged that state and local governments, the institutions within reach of their authority, and all private organizations adopt the safeguard requirements by whatever means are appropriate.

Revolutionary changes in data collection, storage and sharing were described by Senator Goldwater, who was one of many witnesses who called for enactment of the recommendations of the HEW Advisory Committee. He stated:

"Computer storage devices now exist which make it entirely practicable to record thousands of millions of characters of information, and to have the whole of this always available for instant retrieval . . . Distance is no obstacle. Communications circuits, telephone lines, radio waves, even laser beams, can be used to carry information in bulk at speeds which can match the computer's own. Time-

[1] *Records, Computers, and the Rights of Citizens*, U.S. Department of Health, Education and Welfare, 1973, p. xx.

sharing is normal . . . we are now hearing of a system whereby it is feasible for there to be several thousands of simultaneous users or terminals. Details of our health, our education, our employment, our taxes, our telephone calls, our insurance, our banking and financial transactions, pension contributions, our books borrowed, our airline and hotel reservations, our professional societies, our family relationships, all are being handled by computers right now. Unless these computers, both governmental and private, are specifically programmed to erase unwanted history, these details from our past can at any time be reassembled to confront us . . . We must program the programmers while there is still some personal liberty left."

The Committee has found that the concern for privacy is a bipartisan issue and knows no political boundaries. President Ford, as Vice-President, chaired a Domestic Council Committee on the Right of Privacy which was established by President Nixon in February 1974. In a recent address on the subject, he stated:

"In dealing with troublesome privacy problems, let us not, however, scapegoat the computer itself as a Frankenstein's monster. But let us be aware of the implications posed to freedom and privacy emerging from the ways we use computers to collect and disseminate personal information. A concerned involvement by all who use computers is the only way to produce standards and policies that will do the job. It is up to us to assure that information is not fed into the computer unless it is relevant.

"Even if it is relevant, there is still a need for discretion. A determination must be made if the social harm done from some data outweighs its usefulness. The decisionmaking process is activated by demands of people on the government and business for instant credit and instant services. Computer technology has made privacy an issue of urgent national significance. It is not the technology that concerns me but its abuse. I am also confident that technology capable of designing such intricate systems can also design measures to assure security."

FEDNET

In the same address, the Vice-President called attention to FEDNET and problems involved in a proposed centralization of computer facilities which concerned several Congressional committees and which provisions in S. 3418 would correct. He stated:

"The Government's General Services Administration has distributed specifications for bids on centers throughout the country for a massive new computer network. It would have the potential to store comprehensive data on individuals and institutions. The contemplated system, known as FEDNET, would link Federal agencies in a network that would allow GSA to obtain personal information from the files of many Federal departments. It is portrayed as the largest single governmental purchase of civilian data communication in history.

"I am concerned that Federal protection of individual privacy is not yet developed to the degree necessary to prevent FEDNET from being used to probe into the lives of individuals. Before building a nuclear reactor, we design the safeguards for its use. We also require environmental impact statements specifying the anticipated effect of the reactor's operation on the environment. Prior to approving a vast computer network affecting personal lives, we need a comparable privacy impact statement. We must also consider the fallout hazards of FEDNET to traditional freedoms."

EXAMPLES

The revelations before the Select Committee to Investigate Presidential Campaign Activities concerning policies and practices of promoting the illegal gathering, use or disclosure of information on Americans who disagreed with governmental policies were cited by almost all witnesses as additional reasons for immediate congressional action on S. 3418 and other privacy legislation. The representative of the American Civil Liberties Union stated:

"Watergate has thus been the symbolic catalyst of a tremendous upsurge of interest in securing the right of privacy: wiretapping and bugging political opponents, breaking and entering, enemies lists, the Huston plan, national security justifications for wiretapping and burglary, misuse of information compiled by government agencies for political purposes, access to hotel, telephone and bank records; all of these show what government can do if its actions are shrouded in secrecy and its vast information resources are applied and manipulated in a punitive, selective, or political fashion."

Despite such current concern, Congressional studies and complaints to Congress show that the threats to individual privacy from the curiosity of administrators and salacious inquiries of investigators predated "Watergate" by many years. These have been described at length in the hearing record on S. 3418.

For example, under pain of civil and criminal sanctions, many people have been selected and told to respond to questions on statistical census questionnaires such as the following:

How much rent do you pay?

Do you live in a one-family house?

If a woman, how many babies have you had? Not counting still births.

How much did you earn in 1967?

If married more than once, how did your first marriage end?

Do you have a clothes dryer?

Do you have a telephone, if so, what is the number?

Do you have a home food freezer?

Do you own a second home?

Does your TV set have UHF?

Do you have a flush toilet?

Do you have a bathtub or shower?

The studies show that thousands of questionnaires are sent out yearly asking personal questions, but people are not told their responses are voluntary; many think criminal penalties attach to them; it is difficult for them to find out what legal penalties attach to a denial of the information or what will be done with it. If they do not respond, reports show that they are subjected to telephone calls, certified follow-up letters, and personal visits. Much of this work is done by the Census Bureau under contract, and many people believe that whatever agency receives the responses, their answers are subject to the same mandatory provisions and confidentiality rules as the decennial census replies. A Senate survey revealed that in 3 years alone the Census Bureau had provided their computer services at the request of 24 other agencies and departments for conducting voluntary surveys covering over 6 million people. Other independent voluntary surveys were conducted by the agencies themselves on subjects ranging from bomb shelters, to smoking habits, to birth control methods, to whether people who had died had slept with the window open. The form usually asked for social security number, address and phone number.

One such survey technique came to light through complaints to Congress from elderly, disabled or retired people in all walks of life who were pressured to answer a 15-page form sent out by the Census Bureau for the Department of Heath, Education and Wefare which asked:

What have you been doing in the last 4 weeks to find work?

Taking things all together, would you say you are very happy, pretty happy, or not too happy these days?

Do you have any artificial dentures?

Do you—or your spouse—see or telephone your parents as often as once a week?

What is the total number of gifts that you give to individuals per year?

How many different newspapers do you receive and buy regularly?

About how often do you go to a barber shop or beauty salon?

What were you doing most of last week?

Applicants for Federal jobs in some agencies and employees in certain cases, have been subjected to programs requiring them to answer forms of psychological tests which contained questions such as these:[2]

I am seldom troubled by constipation.

My sex life is satisfactory.

At times I feel like swearing.

I have never been in trouble because of my sex behavior.

I do not always tell the truth.

I have no difficulty in starting or holding my bowel movements.

I am very strongly attracted by members of my own sex.

I like poetry.

I go to church almost every week.

I believe in the second coming of Christ.

---

[2] Senate Report 93–724, to accompany S. 1688, "To Protect the Privacy and Rights of Federal Employees." The report describes other similar programs for soliciting, collecting or using personal information from and about applicants and employees. S. 1688 has been approved by the Senate five times.

I believe in a life hereafter.
My mother was a good woman.
I believe my sins are unpardonable.
I have used alcohol excessively.
I loved my Mother.
I believe there is a God.
Many of my dreams are about sex matters.
At periods my mind seems to work more slowly than usual.

I am considered a liberal "dreamer" of new ways rather than a practical follower of well-tried ways. (a) true, (b) uncertain, (c) false.

When telling a person a deliberate lie, I have to look away, being ashamed to look him in the eye. (a) true, (b) uncertain, (c) false.

FIRST AMENDMENT PROGRAMS: THE ARMY

Section 201(b)(7) prohibits departments and agencies from undertaking programs for gathering information on how people exercise their First Amendment rights. Section 201(a) prevents them from collecting and maintaining information which is not relevant to a statutory purpose.

The need for these provisions have been made evident in many ways. In addition to federal programs for asking people questions such as whether they "believe in the second coming of Christ," there have been numerous other programs affecting First Amendment rights.

One of the most pervasive of the intrusive information programs which have concerned the Congress and the public in recent years involved the Army surveillance of civilians, through its own records and those of other federal agencies. The details of these practices have been documented in Congressional hearings and reports and where summarized by Senator Ervin as follows:[3]

Despite First Amendment rights of Americans, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.

"Allegedly for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, taperecorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

"With very few, if any, directives to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

"This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.

"The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks."

Mr. HUDDLESTON. Mr. President, as a member of the Government Operations Committee, I am pleased to support S. 3418, which is designed to protect the right of privacy of individual citizens in the collection, maintenance and dissemination of personal information.

---

[3] *Hearings* before the Subcommittee on Constitutional Rights of the Judiciary Committee, 4 *Columbia Human Rights Review* (1972) Hearings, 92d Cong., 2d sess. February 1971.

The right of individual privacy is vital to any free society.

That right is a basic concept which permeates the very fiber of our Constitution, even though it is not an explicit constitutional guarantee. The freedoms guaranteed by the first amendment—free speech, a free press, and freedom of assembly and religion—at the very least imply the right to be "let alone" by the Government. The principle is further demonstrated by the constitutional prohibition against the Government invading the privacy of homes or businesses by conducting unreasonable search and seizure and the right against self-incrimination is another section that deals with privacy.

The individual's right to privacy has long been recognized by the courts which have consistently protected it from both governmental and nongovernmental intervention. As technological advances—cameras, wiretaps, sound recordings, and so forth—provided new opportunities for infringement upon these rights, the courts responded in an affirmative manner. Unfortunately, due to the nature of the courts, this response has often been slow and incomplete. Case law is built gradually over a period of years and is often incomplete because it is usually decided on narrow issues of law. Thus, what is needed now is a coordinated and comprehensive approach to the problems that can be provided only by the Congress.

Technology is again advancing, this time in the form of computers. This new technology brings with it, as advancements often do, the possibility for negligent use or deliberate misuse. This is what we must guard against. With the development of the computer it has become possible to collect, instantly retrieve and analyze vast amounts of personal information. Access to this personal data has been expanded by the computer's ability to retrieve data across agency, institutional, governmental and geographic boundaries.

A prime example of the type of advanced computer system we may be dealing with in the future is the proposed FEDNET. This giant computerized information system, brainchild of the General Services Administration, was designed to centralize the data processing and telecommunications operations of numerous Federal agencies. Without proper safeguards, vast amounts of personal information retained by the various agencies would be instantly available at hundreds of terminals scattered throughout the United States. And that information covers every spectrum—educational, medical, financial and judicial—of the lives of hundreds of thousands of private citizens. Fortunately this system has been temporarily sidetracked. But the threat of "Big Brother" was clearly there.

Our recent experience with Watergate and related matters points up the need for enacting safeguards to protect the collection and use of such information. The compilation of an enemies list, for example, must be viewed as only the first step in an abuse of power, for the next logical step would be the compilation of "useful" information about those on the list. And what more ready source exists than the bulging files of the Federal Government.

The need for protective legislation is well documented. The record is replete with calls for safeguards in this area. Congress has been probing this problem for years with the leadership of such members as the distinguished Senator from North Carolina (Mr. Ervin). In

June of this year, the Committee on Government Operations ad hoc Subcommittee on Privacy and Information Systems in conjunction with the Judiciary Committee's Subcommittee on Constitutional Rights conducted hearings on S. 3418. The roster of witnesses included high ranking civil servants and recognized nongovernment experts. The general consensus of those testifying was that there is a definite need to protect individual privacy in this area. Former Attorney General Elliot Richardson, for example, stated at those hearings:

> I certainly hope . . . a major bill will be enacted to establish in law the fundamental principles of fair information practice that are necessary to safeguard the right of personal privacy as it relates to record keeping about individual Americans.

Several major studies drew the same conclusion.

The HEW Advisory Committee on Automated Personal Data Systems issued its report, "Records, Computers, and The Rights of Citizens," in 1973. This committee determined that under current law, a person's privacy is not adequately protected against arbitrary or abusive recordkeeping practices and that there is a need to establish standards of recordkeeping practices which are appropriate to the computer age.

Another study, made by the Judiciary Committee's Subcommittee on Constitutional Rights, entitled "Federal Data Banks and Constitutional Rights," produced some sobering statistics. Agencies maintaining 84 percent of the Federal data banks analyzed—858—were unable to cite explicit statutory authority for their existence and 18 percent could not cite any statutory authority.

While the actual and potential abuses of personal information systems have been well documented, we should not view all such systems as sinister threats to personal privacy. Information regarding private individuals is a vital element of any government. Officials must have certain information and statistics if they are to devise and implement programs and policies which fit the needs of the people. This requires the collection, analysis, and dissemination of some personal information. Most agencies accomplish this without infringing upon individual rights. However, the need for safeguards is not negated by this. The threat still exists and must be dealt with.

I believe that S. 3418 would promote accountability and responsibility in Federal agencies by establishing minimum standards for gathering, handling, and processing personal information by Federal departments and agencies. Only information that is relevant and necessary for a statutory purpose of the agency could be collected, solicited, and maintained.

Furthermore, information would have to be accurate, complete, timely, and relevant to the agencies' needs. Disclosure of information could only be made under certain defined conditions.

With some necessary exceptions—for example, if national defense would be endangered—an individual would be allowed to review his or her files and challenge the content. To enforce his or her rights under the act, the individual would have access to the courts.

A significant feature of the bill is the creation of the Privacy Protection Commission to assist agencies in complying with the letter and spirit of the act; investigate abuses; and make recommendations to

Congress regarding the need for additional legislation to protect individual privacy in a computer age. The Commission would also compile an annual directory of Federal personal information files such as those maintained on civilians by the military several years ago.

There even would be some relief for those who find themselves inundated with unwanted or junk mail. An individual could have his or her name removed from a mailing list.

I believe that the time to act on this matter is now. Delay may well be costly in terms of freedoms lost and increased financial burdens.

Dr. Alan Westin, professor of public law and government, Columbia University, has warned in his testimony before the Committee on Government Operations, that a delay will assure that a large number of major data systems will be built in ways that will make it extremely expensive to alter the software, change the file structures or reorganize the data flows. Let us not delay at our own expense.

Mr. Baker. Mr. President, it is my privilege to join my colleagues from North Carolina (Mr. Ervin), Illinois (Mr. Percy), Maine (Mr. Muskie), Connecticut (Mr. Ribicoff), Washington (Mr. Jackson), and Arizona (Mr. Goldwater) in cosponsoring S. 3418, the so-called privacy bill.

I think it is fair to term S. 3418 a "privacy" bill because it seeks to reduce, if not eliminate, the peril to personal privacy and individual rights presented by governmental data banks and information gathering systems. Moreover, traveling in the wake of the recent disclosures of the dubious uses to which Internal Revenue Service files, FBI data banks, and military information systems have been directed, and in light of the massive information recording facilities possessed by other Federal agencies, privacy legislation designed to effect fair information practices and to provide for a single mission oversight and clearinghouse Privacy Protection Commission is particularly appropriate.

As an advocate of increased congressional and Presidential oversight of Federal intelligence gathering, surveillance, and law enforcement agencies, I believe that an independent Privacy Protection Commission, as proposed by S. 3418, will facilitate legislative and executive oversight through creating a central clearinghouse for ascertaining the character and existence of all Federal information systems and by bearing a positive responsibility to monitor governmental data system procedures and policies. Perhaps more importantly, title II of S. 3418 outlines Federal standards governing the gathering and distribution of information relating to U.S. citizens and permanent resident aliens. These standards affirm that the existence of governmental recordkeeping systems should be public knowledge; that governmental agencies should maintain only such records as are related to and permitted by its statutory authority; that Federal information systems containing personal data are accurate, relevant, and complete; that personal files be kept secure and confidential; and that interagency pooling or transfers of personal data be recorded, disclosed, and relevant to the needs of the agency to which the information is transferred. The standards provided in title II of the bill also strictly limit the collection of information regarding a citizen's exercise of his first amendment rights—thereby reaching the concern produced by ongoing revelations of FBI, IRS, and military compilations of information concerning dissident or political action groups.

To those of my colleagues who may be concerned regarding the impact of S. 3418 upon the intelligence and law-enforcement community, I would note that section 203 of the bill provides responsible foreign policy, national defense, and law enforcement related exemptions from the bill's personal information disclosure requirements, disclosure of the source of personal information, and the right of the individual to be informed of the existence of personal information on file. It should be emphasized that the standards and sanctions imposed by S. 3418 pertain only to personal information regarding American citizens and resident aliens and should not impair the ability of U.S. intelligence agencies to collect and keep confidential information regarding foreign agents and nonresident aliens.

Senate passage, and I hope it will pass, of this privacy bill should not be construed as imputing any unworthy motives to the executive branch or the officials of Federal agencies currently involved in information collection and data bank operations. What this bill is designed to do is to limit personal data collection to a necessary minimum, to apprise the citizenry of the existence and character of all governmental data systems, to insure that data collection does not impair individual constitutional rights, and to provide the public with an awareness of how much and under what authority personal information is being assembled and assimilated by the Federal Government.

Mr. RIBICOFF. Mr. President, 41 years ago, George Bernard Shaw, in a speech, commented:

> There is no such thing as privacy in this country.

Unfortunately, the statement remains true today.

Over the past two decades, the computer has allowed the Government to expand its information-gathering facilities. In 1972, the National Academy of Sciences reported:

> That is technologically possible today, especially with recent advances in mass storage memories, to build a computerized, on-line file containing the compacted equivalent of 20 pages of typed information about the personal history of selected activities of every man, woman, and child in the United States, arranging the system so that any single record could be retrieved in about 30 seconds.

This possibility requires that we ask a fundamental question about the rights of the individual citizen in our society. Is it in our best interests to allow the Government to continue to expand its files on citizens and to gather detailed information on any citizen without proper safeguards for the privacy of those individuals?

As early as 1967, the Senate Administrative Practices Subcommittee revealed that—

> Our names alone are in government files 2,800 million times. Our social security numbers are listed 2,800 million times. Police records number 264,500 million; medical histories, 342 million; and psychiatric histories 279 million.

The Federal Government now maintains over 800 data-collection systems. These data systems contain over 1 billion records on individuals. Yet, of the over 800 Federal data collection systems, only 10 percent are specifically authorized by law—more than 40 percent do not inform individuals that records are being kept on them—half the systems do not permit individuals to review or correct their own files.

Today, the Government maintains "files" on a large majority of Americans. Often, these files contain information of a most personal

nature. Often the information is outdated and incorrect. Yet, decisions affecting people's lives are made based on these same files. It appears that a large and unmeasured toll appears to be taken on the constitutional principles of accountability, responsibility, and limited government.

Both the Republican and Democratic policy platforms have placed privacy as a high priority concern. President Ford, in his speech before the joint session of Congress on August 12, 1974, commented:

> There will be hot pursuit of tough laws to prevent illegal invasions of privacy in both government and private activities.

The HEW Advisory Committee on Automated Personal Data Systems recommended the enactment of a Federal "Code of Fair Information Practice," based on five basic principles, for all automated personal data systems. The principles are incorporated into the individual rights guaranteed in S. 3418, the bill before us today, which I am pleased to be a sponsor:

To know that no secret data system exists;

To know what information about that individual is in a record and how it is used;

To prevent information obtained for one purpose from being used for other purposes without consent of the individual; and

To correct or amend information about that individual.

S. 3418 establishes an independent Privacy Protection Commission to deal systematically with the range of administrative and technological problems throughout Federal Government agencies and to study privacy abuses in the private sector as well as in State and local government agencies. The commission will serve as an effective balance between citizens and the Government in order to further develop policy in our rapidly changing technological environment. There is a need for a staff of experts to furnish assistance to Government agencies and to inform Congress and the public of the scope and kinds of data-handling used by Government and private organizations. The commission would continually check the need for new or expanded data systems and provide citizens with adequate information about which agencies maintain, distribute, or use information about them.

The bill requires that an individual be informed when a file is kept on him and that he be given an opportunity to challenge information in the file. The bill requires that all files be regularly updated, that information be disclosed only in accord with strict guidelines, and that records be kept of all such disclosures.

New advances in computer technology doubtless provide our society with advantages. Our technology allows Government and industry to operate more efficiently and cheaply. It allows quick access to information—information that becomes too easily available. We would be foolish to contend that the computer presents us with no dangers. We would be wrong not to consider the very real threats presented by loosely controlled or unregulated computer data systems. I believe S. 3418 is a necessary check on Government data systems.

Justice Brandeis' wisdom in his dissenting opinion in the first wiretap case to reach the Supreme Court, *Olmstead* v. *United States* (1927), in crediting the framers of the Constitution with having "conferred, as against the Government, the right to be left alone—the most com-

prehensive of rights and the right most valued by civilized man" must be remembered. He urged that privacy must be protected by nothing less than the prevention of "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed."

No specific statute allowed the Army to blacklist persons involved in the antiwar movement. No act of Congress authorized the Army to send the names of blacklisted persons to numerous State and Federal agencies. Congress never intended that persons be subjected to surveillance and intimidation, because they chose to exercise their first amendment rights.

I lend my support to S. 3418 and will vote for its passage.

Mr. ROBERT C. BYRD. Mr. President, I ask unanimous consent that the names of Mr. Cranston and Mr. Nelson be added as cosponsors of the bill under consideration (S. 3418) to establish a Federal Privacy Board.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. ERVIN. Mr. President, I commend the distinguished Senator from Connecticut (Mr. Ribicoff) for the great contribution which he has made to the development of this bill.

The PRESIDING OFFICER. The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed for a third reading and was read the third time.

The PRESIDING OFFICER. The question is, Shall the bill pass?

The yeas and nays have been ordered, and the clerk will call the roll.

The legislative clerk called the roll.

Mr. ROBERT C. BYRD. I announce that the Senator from Texas (Mr. Bentsen), the Senator from Mississippi (Mr. Eastland), the Senator from Arkansas (Mr. Fulbright), the Senator from South Dakota (Mr. McGovern), the Senator from Minnesota (Mr. Mondale), the Senator from New Mexico (Mr. Montoya), the Senator from Maine (Mr. Muskie), the Senator from Rhode Island (Mr. Pastore), the Senator from Alabama (Mr. Sparkman), and the Senator from Missouri (Mr. Symington) are necessarily absent.

I further announce that the Senator from Minnesota (Mr. Humphrey) is absent on official business.

I further announce that, if present and voting, the Senator from Minnesota (Mr. Humphrey), the Senator from Rhode Island (Mr. Pastore), and the Senator from Missouri (Mr. Symington) would each vote "yea."

Mr. GRIFFIN. I announce that the Senator from Utah (Mr. Bennett), the Senator from Colorado (Mr. Dominick), and the Senator from Arizona (Mr. Fannin) are necessarily absent.

I also announce that the Senator from New York (Mr. Buckley) and the Senator from Maryland (Mr. Mathias) are absent on official business.

I further announce that the Senator from Oregon (Mr. Hatfield) is absent due to illness in the family.

I further announce that, if present and voting, the Senator from Oregon (Mr. Hatfield) would vote "yea."

63-619—76——54

The result was announced—yeas 74, nays 9, as follows:

[No. 496 Leg.]

YEAS—74

Abourezk	Fong	Metzenbaum
Allen	Goldwater	Moss
Baker	Gravel	Nelson
Bartlett	Griffin	Nunn
Bayh	Gurney	Packwood
Beall	Hart	Pearson
Bellmon	Hartke	Pell
Bible	Haskell	Percy
Biden	Hathaway	Proxmire
Brock	Helms	Randolph
Brooke	Hollings	Ribicoff
Burdick	Huddleston	Roth
Byrd, Harry F., Jr.	Hughes	Schweiker
Byrd, Robert C.	Inouye	Scott, Hugh
Cannon	Jackson	Stafford
Case	Javits	Stennis
Chiles	Johnston	Stevens
Church	Kennedy	Stevenson
Clark	Long	Taft
Cook	Magnuson	Talmadge
Cranston	Mansfield	Tunney
Dole	McClure	Weicker
Domenici	McGee	Williams
Eagleton	McIntyre	Young
Ervin	Metcalf	

NAYS—9

Aiken	Hansen	Scott, William L.
Cotton	Hruska	Thurmond
Curtis	McClellan	Tower

NOT VOTING—17

Bennett	Fulbright	Montoya
Bentsen	Hatfield	Muskie
Buckley	Humphrey	Pastore
Dominick	Mathias	Sparkman
Eastland	McGovern	Symington
Fannin	Mondale	

So the bill (S. 3418) was passed.[1]

[From the Congressional Record—Senate, Nov. 22, 1974]

SENATE CONSIDERS H.R. 16373; SUBSTITUTES TEXT OF S. 3418

Mr. ERVIN. Mr. President, I move that the Chair lay before the Senate the message from the House of Representatives on H.R. 16373.

The motion was agreed to; and the Presiding Officer (Mr. Stevenson) laid before the Senate H.R. 16373, an act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, which was read twice by its title.

---

[1] See p. 334.

Mr. ERVIN. This is the House-passed bill on privacy. The Senate has passed its own bill. I move to strike out everything in H.R. 16373 after the enacting clause, and to substitute therefor the text of the Senate version of the privacy bill (S. 3418) as passed by the Senate yesterday.

The motion was agreed to.

The PRESIDING OFFICER. The question is on the engrossment of the amendment and third reading of the bill.

The amendment was ordered to be engrossed, and the bill to be read a third time.

The bill (H.R. 16373) was read the third time, and passed.[1]

[From the Congressional Record—Senate, Dec. 17, 1974]

SENATE CONSIDERS HOUSE SUBSTITUTE OF TEXT OF H.R. 16373 TO S. 3418 AND ADOPTS COMPROMISE AMENDMENTS IDENTICAL TO THOSE CONSIDERED IN HOUSE

Mr. ERVIN. Mr. President, I ask the Chair to lay before the Senate a message from the House of Representatives on S. 3418.

The Presiding Officer laid before the Senate the amendments of the House of Representatives to the bill (S. 3418) to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes, as follows:

Strike out all after the enacting clause, and insert: That this Act may be cited as the "Privacy Act of 1974".

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

---

[1] See p. 334.

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful, arbitrary, or capricious action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any collection or grouping of information about an individual that is maintained by an agency and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual; and

"(6) the term 'statistical research or reporting record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) for a routine use described under subsection (e)(2)(D) of this section;

"(3) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(4) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(5) to the National Archieves of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(6) to another agency to to any instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(7) to a person who is actively engaged in saving the life of such individual, if upon such disclosure notification is transmitted to the last known address of such individual;

"(8) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any such joint committee; or

"(9) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsection (b)(1) of this section or disclosures to the public from records which by law or regulation are open to public inspection or copying, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(6) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency within two years preceding the making of the correction of the record of the individual, except that this paragraph shall not apply to any record that was disclosed prior to the effective date of this section or for which no accounting of the disclosure is required.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him to review the record and have a copy made of all or any portion thereof in a form comprehensible to him;

"(2) permit the individual to request amendment of a record pertaining to him and either—

"(A) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(B) promptly inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review by the agency of that refusal, and the name and business address of the official within the agency to whom the request for review may be taken;

"(3) permit any individual who disagrees with the refusal of the agency to amend his record to request review of the refusal by the official named in accordance with paragraph (2)(B) of this subsection; and if, after the review, that official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency;

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and, upon request, provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) which Federal statute or regulation, if any, requires disclosure of the information;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) other purposes for which the information may be used, as published pursuant to paragraph (2)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

"(2) subject to the provisions of paragraph (5) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine purpose for which the records contained in the system are used or intended to be used, including the categories of users of the records for each such purpose;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; and

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content;

"(3) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(4) maintain no record concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained: *Provided, however*, That the provisions of this paragraph shall not be deemed to prohibit the maintenance of any record of activity which is pertinent to and within the scope of a duly authorized law enforcement activity; and

"(5) at least 30 days prior to publication of information under paragraph (2)(D) of this subsection published in the Federal Register notice of the use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

"(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means the head of the agency may deem necessary for each individual to be able to exercise fully his rights under this section; and

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(2) of this section in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency (A) refuses to comply with an individual request under subsection (d)(1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to secure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of records and consequently a determination is made which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

"(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(3) In any suit brought under the provisions of subsection (g)(1)(B) or (C) of this section in which the court determines that the agency acted in a manner which was willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—

"(A) actual damages sustained by the individual as a result of the refusal or failure; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(4) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) CRIMINAL PENALTIES.—Any officer or employee of the United States, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be fined not more than $5,000.

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from any part of this section except subsections (b) and (e)(2)(A) through (F) and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to ap-

prehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(2) (G) and (H), and (f) of this section if the system of records is—

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however*, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

"(4) required by statute to be maintained and used solely as statistical research or reporting records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

"(l)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of his section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be subject to all provisions of this section except subsections (c)(4); (d) (2), (3), and (4); (e)(1), (2)(H) and (3); (f)(4); (g)(1) (B) and (C), and (3).

"(m)(1) MORATORIUM ON THE USE OF THE SOCIAL SECURITY ACCOUNT NUMBER.—No Federal agency, or any State or local government acting in compliance with any Federal law or federally assisted program, shall deny any individual any right, benefit, or privilege provided by law by reason of such individual's refusal to disclose his social security account number.

"(2) This subsection shall not apply—

"(A) with respect to any system of records in existence and operating prior to January 1, 1975; and

"(B) when disclosure of a social security account number is required by Federal law.

"(3) No Federal agency, or any State or local government acting in compliance with any Federal law or federally assisted program, shall use the social security account number for any purpose other than for verification of the identity of an individual unless such other purpose is specifically authorized by Federal law.

"(n) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.".

SEC. 4. The chapter analysis of chapter 5 of title 5, United States Code, is amended by inserting:

"552A. RECORDS ABOUT INDIVIDUALS."

immediately below:

"552. PUBLIC INFORMATION; AGENCY RULES, OPINION, ORDERS, AND PROCEEDINGS.".

SEC. 5. The amendments made by this Act shall become effective on the one hundred and eightieth day following the date of enactment of this Act.

Amend the title so as to read: "An act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies."

Mr. ERVIN. Mr. President, on November 21, just before the Thanksgiving recess, both the Senate and the House adopted in different forms——

The PRESIDING OFFICER. Will the Senator suspend briefly until the Chair gets order in the Senate.

I would like to ask the Members of the Senate to please bring order to the Chamber because the Senator from North Carolina is entitled to be heard and he cannot be heard. Would those members conversing please remove themselves to the cloakroom.

The Senator will continue to suspend until there is order in the Chamber.

The Senator may proceed.

Mr. ERVIN. On November 21, just before the Thanksgiving recess, both the Senate and the House passed in different forms Federal privacy legislation. Because of the limited amount of time available between the time of the reconvening of Congress after the recess and the end of the session of Congress members of the Government Operations

Committee of the Senate and the House agreed that they would have the different versions studied by their respective staffs during the recess.

After the recess the members of the staffs who had made this study reported to the members of the two committees, and after that the members of the two committees met informally and agreed on the amendments that I will offer in behalf of all the original cosponsors of the privacy bill.

We thought this was a better way of doing it without having a conference and I have been assured by the members of the House Government Operations Committee interested in privacy legislation, that the House will accept these amendments which I propose on behalf of myself and all of the original cosponsors of the bill.

The main differences between the two versions which are reconciled here was that instead of establishing a privacy board, as the Senate bill did, that we will have a privacy study commission to study the subject and report back to the President, to the Senate, and to the House.

We also eliminated, in deference to the House, provisions of the bill dealing with the private sector and we also eliminated some of the provisions dealing with law enforcement agencies.

Now, Mr. President, on behalf of the original cosponsors of the Senate bill and myself, I make this motion.

Mr. President, I move that the Senate agree to the engrossed amendments of the House to the bill (S. 3418) to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes, with the following amendments to such engrossed amendments:

In lieu of the matter proposed to be inserted by the House to the text of the bill, insert the following amendment which I now send to the desk.

The PRESIDING OFFICER. The amendment will be stated.

The assistant legislative clerk proceeded to read the amendment.

Mr. ERVIN. Mr. President, I ask unanimous consent that further reading of the amendment be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendment is as follows:

In lieu of the matter proposed to be inserted by the House to the text of the bill, insert the following:

That this Act may be cited as the "Privacy Act of 1974".

SEC. 2. (a) The Congress finds that—

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to—

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or international action which violates any individual's rights under this Act.

SEC. 3. Title 5, United States Code, is amended by adding after section 552 the following new section:

"§ 552a. Records maintained on individuals

"(a) DEFINITIONS.—For a purposes of this section—

"(1) the term 'agency' means agency as defined in section 552(e) of this title;

"(2) the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;

"(3) the term 'maintain' includes maintain, collect, use, or disseminate;

"(4) the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

"(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

"(6) the term 'statistical record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13.

"(7) the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

"(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

"(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

"(2) required under section 552 of this title;

"(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

"(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

"(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

"(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

"(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

"(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

"(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

"(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

"(11) pursuant to the order of a court of competent jurisdiction.

"(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

"(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

"(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) the name and address of the person or agency to whom the disclosure is made;

"(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

"(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

"(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

"(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

"(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

"(2) permit the individual to request amendment of a record pertaining to him and—

"(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

"(B) promptly, either—

"(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer desig-

nated by the head of the agency, and the name and business address of that official;

"(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing officials' determination under subsection (g)(1)(A) of this section;

"(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

"(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

"(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

"(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

"(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

"(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

"(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

"(B) the principal purpose or purposes for which the information is intended to be used;

"(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

"(D) the effects on him, if any, of not providing all or any part of the requested information;

"(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—

"(A) the name and location of the system;

"(B) the categories of individuals on whom records are maintained in the system;

"(C) the categories of records maintained in the system;

"(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

"(F) the title and business address of the agency official who is responsible for the system of records;

"(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

"(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

"(I) the categories of sources of records in the system;

"(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, time-

liness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

"(6) prior to disseminating any record about an individual to any person other than an agency, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant;

"(7) maintain no record describing how any individual exercises rights guaranteed by the first amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within thes scope of an authorized law enforcement activity;

"(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

"(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

"(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarassment, inconvenience, or unfairness to any individual on whom information is maintained; and

"(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

"(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

"(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

"(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

"(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

"(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

"(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

"(g)(1) CIVIL REMEDIES.—Whenever any agency—

"(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

"(B) refuses to comply with an individual request under subsection (d)(1) of this section;

"(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in my determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

"(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisons of this subsection.

"(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

"(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complaint has substantially prevailed.

"(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

"(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

"(B) the costs of the action together with reasonable attorney fees as determined by the court.

"(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to the establishment of the liability of the agency to the individual under this section, the action may be bought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

"(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of the section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

"(i)(1) CRIMINAL PENALTIES.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this secton or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

"(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

"(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of section 553(b)

(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1), (2), and (4), (e)(4)(A) through (F)(e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

"(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2) and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) of this section if the system of records is—

"(1) subject to the provisions of section 552(b)(1) of this title;

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however*, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

"(4) required by statute to be maintained and used solely as statistical records;

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity of fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

"(l) (1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

"(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (a) (4) (A) through (G) of this section) shall be published in the Federal Register.

"(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e) (4) (A) through (G) and (e) (9) of this section.

"(m) GOVERNMENT CONTRACTORS.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

"(n) MAILING LISTS.—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

"(o) REPORT ON NEW SYSTEMS.—Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

"(p) ANNUAL REPORT.—The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

"(q) EFFECT OF OTHER LAWS.—No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.".

SEC. 4. The chapter analysis chapter 5 of title 5, United States Code, is amended by inserting:

"552A. RECORDS ABOUT INDIVIDUALS."

immediately below:

"552. PUBLIC INFORMATION; AGENCY RULES, OPINIONS, ORDERS, AND PROCEEDINGS."

SEC. 5. (a) (1) There is established a Privacy Protection Study Commission (hereinafter referred to as the "Commission") which shall be composed of seven members as follows:

(A) three appointed by the President of the United States.

(B) two appointed by the President of the Senate, and

(C) two appointed by the Speaker of the House of Representatives.

Members of the Commission shall be chosen from among persons who, by reason of their knowledge and expertise in any of the following areas—civil rights and liberties, law, social sciences, computer technology, business, records management, and State and local government—are well qualified for service on the Commission.

(2) The members of the Commission shall elect a Chairman from among themselves.

(3) Any vacancy in the membership of the Commission, as long as there are four members in office, shall not impair the power of the Commission but shall be filled in the same manner in which the original appointment was made.

(4) A quorum of the Commission shall consist of a majority of the members, except that the Commission may establish a lower number as a quorum for the purpose of taking testimony. The Commission is authorized to establish such committees and delegate such authority to them as may be necessary to carry out its functions. Each member of the Commission, including the Chairman, shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information necessary to the performance of their functions, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or a member designated by the Chairman to be acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress, Government agencies, other persons, and the public, and, on behalf of the Commission, shall see to the faithful execution of the administrative policies and decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

(5)(A) Whenever the Commission submits any budget estimate or request to the President or the Office of Management and Budget, it shall concurrently transmit a copy of that request to Congress.

(B) Whenever the Commission submits any legislative recommendations, or testimony, or comments on legislation to the President or Office of Management and Budget, it shall concurrently transmit a copy thereof to the Congress. No officer or agency of the United States shall have any authority to require the Commission to submit its legislative recommendations, or testimony, or comments on legislation, to any officer or agency of the United States for approval, comments, or review, prior to the submission of such recommendations, testimony, or comments to the Congress.

(b) The Commission shall—

(1) make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information; and

(2) recommend to the President and the Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

(c)(1) In the course of conducting the study required under subsection (b)(1) of this section, and in its reports thereon, the Commission may research examine, and analyze—

(A) interstate transfer of information about individuals that is undertaken through manual files or by computer or other electronic or telecommunications means;

(B) data banks and information programs and systems the operation of which significantly or substantially affect the enjoyment of the privacy and other personal and property rights of individuals;

(C) the use of social security numbers, license plate numbers, universal identifiers, and other symbols to identify individuals in data banks and to gain access to, integrate, or centralize information systems and files; and

(D) the matching and analysis of statistical data, such as Federal census data, with other sources of personal data, such as automobile registries and telephone directories, in order to reconstruct individual responses to statistical questionnaires for commercial or other purposes, in a way which results

in a violation of the implied or explicitly recognized confidentiality of such information.

(2)(A) The Commission may include in its examination personal information activities in the following areas: medical; insurance; education; employment and personel; credit, banking and financial institutions; credit bureaus; the commercial reporting industry; cable television and other telecommunications media; travel, hotel, and entertainment reservations; and electronic check processing.

(B) The Commission shall include in its examination a study of—

(i) whether a person engaged in interstate commerce who maintains a mailing list should be required to remove an individual's name and address from such list upon request of that individual;

(ii) whether the Internal Revenue Service should be prohibited from transferring individually indentifiable data to other agencies and to agencies of State governments;

(iii) whether the Federal Government should be liable for general damages incurred by an individual as the result of a willful or intentional violation of the provisions of sections 552a (g) (1) (C) or (D) of title 5, United States Code; and

(iv) whether and how the standards for security and confidentiality of records required under section 552a (e) (10) of such title should be applied when a record is disclosed to a person other than an agency.

(C) The Commision may study such other personal information activities necessary to carry out the congressional policy embodied in this Act, except that the Commission shall not investigate information systems maintained by religious organizations.

(3) In conducting such study, the Commission shall—

(A) determine what laws, Executive orders, regulations, directives, and judicial decisions govern the activities under study and the extent to which they are consistent with the rights of privacy, due process of law, and other guarantees in the Constitution;

(B) determine to what extent governmental and private information systems affect Federal-State relations or the principle of separation of powers;

(C) examine the standards and criteria governing programs, policies, and practices relating to the collection, soliciting, processing, use, access, integregation, dissemination, and transmission of personal information; and

(D) to the maximum extent practicable, collect and utilize findings, reports, studies, hearing transcripts, and recommendations of governmental, legislative and private bodies, institutions, organizations, and individuals which pertain to the problems under study by the Commission.

(d) In addition to its other functions the Commission may—

(1) request assistance of the heads of appropriate departments, agencies, and instrumentalities of the Federal Government, of State and local governments, and other persons in carrying out its functions under this Act;

(2) upon request, assist Federal agencies in complying with the requirements of section 552a of title 5, United States Code;

(3) determine what specific categories of information, the collection of which would violate an individual's right of privacy, should be prohibited by statute from collection by Federal agencies; and

(4) upon request, prepare model legislation for use by State and local governments in establishing procedures for handling, maintaining, and disseminating personal information at the State and local level and provide such technical assistance to State and local governments as they may require in the preparation and implementation of such legislation.

(e)(1) The Commission may, in carrying out its functions under this section, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, administer such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. A subpena shall be issued only upon an affirmative vote of a majority of all members of the Commission. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

(2)(A) Each department, agency, and instrumentality of the executive branch of the Government is authorized to furnish to the Commission, upon request made by the Chairman, such information, data, reports and such other assistance as the Commission deems necessary to carry out its functions under this section. Whenever the head of any such department, agency, or instrumentality submits a report pursuant to section 552a(o) of title 5, United States Code, a copy of such report shall be transmitted to the Commission.

(B) In carrying out its functions and exercising its powers under this section, the Commission may accept from any such department, agency, independent instrumentality, or other person any individually identifiable data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall assure that the information is used only for the purpose for which it is provided, and upon completion of that purpose such information shall be destroyed or returned to such department, agency, independent instrumentality, or person from which it is obtained, as appropriate.

(3) The Commission shall have the power to—

(A) appoint and fix the compensation of an executive director, and such additional staff personnel as may be necessary, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, but at rates not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of such title; and

(B) procure temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code.

The Commission may delegate any of its functions to such personnel of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

(4) The Commission is authorized—

(A) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

(B) to enter into contracts or other arrangements or modifications thereof, with any government, any department, agency, or independent instrumentality of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (41 U.S.C. 5);

(C) to make advance, progress, and other payments which the Commission deems necessary under this Act without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529); and

(D) to take such other action as may be necsesary to carry out its functions under this section.

(f)(1) Each member of the Commission who is an officer or employee of the United States shall serve without additional compensation, but shall continue to receive the salary of his regular position when engaged in the performance of the duties vested in the Commission.

(2) A member of the Commission other than one to whom paragraph (1) applies shall receive per diem at the maximum daily rate for GS–18 of the General Schedule when engaged in the actual performance of the duties vested in the Commission.

(3) All members of the Commission shall be reimbursed for travel, subsistence, and other necessary expenses incurred by them in the performance of the duties vested in the Commission.

(g) The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this section. The Commission shall make a final report to the President and to the Congress on its findings pursuant to the study required to be made under subsection (b)(1) of this section not later than two years from the date on which all of the members of the Commission are appointed. The Commission shall cease to exist thirty days after the date on which its final report is submitted to the President and the Congress.

(h)(1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records

which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be fined not more than $5,000.

(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Commission under false pretenses shall be fined not more than $5,000.

SEC. 6. The Office of Management and Budget shall—

(1) develop guidelines and regulations for the use of agencies in implementing the provisions of section 552a of title 5, United States Code, as added by section 3 of this Act; and

(2) provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies.

SEC. 7. (a) (1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) The provisions of paragraph (1) of this subsection shall not apply with respect to—

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

SEC. 8. The provisions of this Act shall be effective on and after the date of enactment, except that the amendments made by sections 3 and 4 shall become effective 270 days following the day on which this Act is enacted.

SEC. 9. There is authorized to be appropriated to carry out the provisions of section 5 of this Act for fiscal year 1975, 1976, and 1977 the sum of $1,500,000, except that not more than $750,000 may be expended during any such fiscal year.

In lieu of the engrossed amendment to the title, insert the following:

Amend the title so as to read: "An Act to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Study Commission, and for other purposes."

Mr. ERVIN. We preserve most of the essential elements of the Senate bill with these few minor changes.

I have been asked by the distinguished Senator from Louisana, as chairman of the Finance Committee, the question whether these amendments would interfere with the practice of the Internal Revenue Service in furnishing information to the State taxing authorities and to congressional committees, and my assurance is that will not be interfered with in any respect whatever.

I would like to address more specifically some other questions raised about how the bill will work with respect to tax information and tax returns. Specifically, the questions relate to the ability of the IRS to disclose tax information under the provision of the bill that allows disclosure for a routine use under a purpose which is compatible with the purpose for which the information is collected.

State and local tax agencies now heavily rely on Federal tax information and investigations when State agencies enforce their tax laws. For example, when the IRS sets up a deficiency against a taxpayer who lives in a State, the IRS frequently sends information on this deficiency to the State, or local, tax agency. The States use this information in collecting their own taxes. This information may be sent before the State itself conducts any tax investigation on the individual.

Under the bill, this is intended to constitute a routine use for a purpose compatible with the purpose for which the information was collected, so the IRS could continue to send this information to the State and local tax agencies as is presently done.

Also, the IRS sends to State, and local, tax agencies the Federal tax returns of individuals who live in the State so the State agency can check to see if the individual has reported the same income and deductions on his Federal and State, or local, tax returns. Again, the States rely on this information in enforcing their own tax laws. Also, this information may be sent to a State before it conducts a tax investigation on its own.

Under the bill, it is intended that this would be a routine use for a purpose compatible with the purpose for which the information is collected so the IRS can continue to send tax information to State and local tax agencies in this way.

The IRS, of course, provides tax information on individuals to the Justice Department when the Justice Department is preparing a tax case against the individual. This information is used by the Justice Department in investigating and preparing tax cases and also is disclosed in court as the Justice Department presents evidence against the individual.

This disclosure both to the Justice Department and in court would represent a routine use of the tax information compatible with the purpose for which it was collected and this disclosure would continue to be possible under the provisions of the bill.

Under the bill tax returns and other tax information can—as under present law—be disclosed to the tax committees of the Congress—the Senate Finance Committee, the House Ways and Means Committee, and the Joint Committee on Internal Revenue Taxation.

Under the bill this information can also continue to be disclosed to the staffs of these committees, as under present law.

Under the bill an agency can disclose tax returns to either House of Congress or to committees of Congress—to the extent of matters within their jurisdiction. Since tax returns can be disclosed by an agency to the Senate and House, it is intended that—as under present law—the committees which have received tax returns can also disclose them to the Senate or House, just as the Joint Committee on Internal Revenue Taxation did with the tax information on President Nixon.

I have also prepared an analysis of these amendments which I submit entitled "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act," which explains the provisions of the amendments.

Mr. President, I ask unanimous consent that this statement be printed at this point in the Record.

There being no objection, the analysis was ordered to be printed in the Record, as follows:

ANALYSIS OF HOUSE AND SENATE COMPROMISE AMENDMENTS TO THE FEDERAL PRIVACY ACT

The establishment of a Privacy Protection Study Commission. Only the Senate bill provided for an oversight and study commission to assist in the implementation of the act and to explore areas concerned with individual privacy which have not been included in the provisions of this legislation. The compromise measure

will establish a Privacy Protection Study Commission of seven members instead of the five provided in the Senate bill. Three of these members will be appointed by the President, two by the President of the Senate, and two by the Speaker of the House of Representatives.

The membership should be representative of the public at large who, by reason of their knowledge and expertise in the areas of civil rights and liberties, law, social sciences, and complete technology, business, and State and local government are well qualified for service on the Commission. While there is no statutory requirement, the Committee could expect that no more than five members of the Commission could be members of one political party.

It is intended that this commission, which will serve for a period of two years, will be solely a study commission. In that capacity it is hoped the commission can assist the Executive Branch and the Congress in their examination of Federal government activities and their impact on privacy as well as representatives of State and local governments and the private sector who are attempting to deal with this important problem.

The scope of the commission's study authority is outlined specifically within the legislation. In subsection (c)(2)(b), the commission is directed to examine certain issues which are not included in the compromise between the House and Senate bill, such as a requirement that a person maintaining mailing lists remove an individual's name upon request; the question of prohibiting the transfer of individually identifiable data from the Internal Revenue Service to other agencies and to Senate governments; a question of whether the Federal government should be liable for general damages occurring from a willful or intentional violation of the provisions of (g)(1), (C) or (D) of this act; and the extent to which requirements for security and confidentiality of records maintained under this act should be applied to a person other than an agency.

The commission shall from time to time and in an annual report, report to the Congress and to the President on its activities, and it shall submit a final report of its findings two years from the date the members of the commission are appointed.

In addition, the commission is authorized to provide necessary technical assistance and prepare model legislation upon request for State and local governments interested in adopting privacy legislation. Strict standards and penalties are placed upon commission members and employees with regard to the handling and unlawful distribution of information about individuals which it receives in the course of carrying out its functions.

While the provisions of the rest of this act do not go into effect until 270 days from the date of enactment, the commission is authorized to go into effect immediately upon the appointment of its members in order that some of its work may be available to the Congress and the Executive Branch by the time the remainder of the legislation becomes effective.

ROUTINE USE

The House bill contains a provision not provided for in the Senate measure exempting certain disclosures of information from the requirement to obtain prior consent from the subject when the disclosure would be for a "routine use." The compromise would define "routine use" to mean: "with respect to the disclosure of a record, the use of such records for a purpose which is compatible with the purpose for which it was collected."

Where the Senate bill would have placed tight restrictions upon the transfer of personal information between or outside Federal agencies, the House bill, under the routine use provision, would permit an agency to describe its routine uses in the Federal Register and then disseminate the information without the consent of the individual or without applying the standards of accuracy, relevancy, timeliness or completeness so long as no determination was being made about the subject.

The compromise definition should serve as a caution to agencies to think out in advance what uses it will make of information. This act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary

exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.

INFORMATION ON POLITICAL ACTIVITIES

The House bill tells agencies that they may not maintain a record concerning the political or religious beliefs or activities of any individual unless maintenance of the record would be authorized expressly by statute or by the individual about whom the record is maintained. The House bill goes on to provide that this subsection is not deemed to prohibit the maintenance of any record or activity which is pertinent to and within the scope of a duly authorized law enforcement activity.

The Senate bill constitutes a prohibition against agency programs established for the purpose of collecting or maintaining information about how individuals exercise First Amendment rights unless the agency head specifically determines that the program is required for the administration of a statute.

The compromise broadens the House provisions application to all First Amendment rights and directs the prohibition against the maintenance of records. However, as in the House bill, it does permit the maintenance, use, collection or dissemination of these records which are expressly authorized by statute or the individual subject or are pertinent to a duly authorized law enforcement activity.

CONFIDENTIAL SOURCES OF INFORMATION

The compromise provision for the maintenance of information received from confidential sources represents an acceptance of the House language after receiving an assurance that in no instance would that language deprive an individual from knowing of the existence of any information maintained in a record about him which was received from a "confidential source." The agencies would not be able to claim that disclosure of even a small part of a particular item would reveal the identity of a confidential source. The confidential information would have to be characterized in some general way. The fact of the item's existence and a general characterization of that item would have to be made known to the individual in every case.

Furthermore, the acceptance of this section in no way precludes an individual from knowing the substance and source of confidential information, should that information be used to deny him a promotion in a government job or access to classified information or some other right, benefit or privilege for which he was entitled to bring legal action when the government wished to base any part of its legal case on that information.

Finally, it is important to note that the House provision would require that all future promises of confidentiality to sources of information be expressed and not implied promises. Under the authority to prepare guidelines for the administration of this act it is expected that the Office of Management and Budget will work closer with agencies to insure that Federal investigators make sparing use of the ability to make express promises of confidentiality.

STANDARDS APPLIED TO DISSEMINATION OUTSIDE THE GOVERNMENT

H.R. 16373 requires that all records which are used by an agency in making any determination about an individual be maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in the determination. S. 3418 goes much further and requires that agencies apply these standards at any time that access is granted to the file, material is added to or taken from the file, or at any time it is used to make a determination affecting the subject of the file.

The difference between these two measures represents a difference in philosophy regarding the handling of personal information. The Senate measure is designed to complement the requirement that agencies maintain only information which is relevant and necessary to accomplish a statutory purpose. The standard of relevancy should be that statutory basis for an information program which is now set forth in (e)(1) of the compromise measure. By adopting this section, the Senate hoped to encourage a periodic review of personal information contained in Federal records as those records were used or disseminated for any purpose.

The House provision would have applied those important standards for maintenance of information in records at any time a determination is made about an

individual. The House bill goes on to permit additional "routine uses" of information which may not rise to the threshhold of an "agency determination" without requiring that the information be upgraded to meet these standards.

The compromise amendment would adopt the section of the House bill applying the standards of accuracy, relevance, timeliness and completeness at the time of a determination. It would add the additional requirement, however, that prior to the dissemination of any record about an individual to any person other than another agency, the sending agency shall make a reasonable effort to assure that the record is accurate, complete, timely, and relevant. This proviso was included because Federal agencies would be governed by a requirement to clean up their records before a determination is made and limited by a requirement to publish each routine use of information in the Federal Register, but the use of information by persons outside the Federal government would not be governed by this act. Therefore, agencies are directed to be far more careful about the dissemination of personal information to persons not governed by the enforcement provisions of this bill.

THE FREEDOM OF INFORMATION ACT AND PRIVACY

Perhaps the most difficult task in drafting Federal privacy legislation was that of determining the proper balance between the public's right to know about the conduct of their government and their equally important right to have information which is personal to them maintained with the greatest degree of confidence by Federal agencies. The House bill made no specific provision for Freedom of Information Act requests of material which might contain information protected by the Privacy Act. Instead, in the committee report on the bill, it recognized that:

"This legislation would have an effect on subsection (b)(6) of the Freedom of Information Act (5 U.S.C., Section 552) which states that the provisions regarding disclosure of information to the public shall not apply to material 'the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.' H.R. 16373 would make all individually identifiable information in government files exempt from public disclosure. Such disclosure could be made available to the public only pursuant to rules published by agencies in the Federal Register permitting the transfer of particular data to persons other than the individuals to whom they pertain."

The committee report went on to express a desire that agencies continue to make certain individually identifiable records open to the public because such disclosure would be in the public interest.

The Senate bill reflected the position of an earlier draft of the House measure in Section 205(b) where it provided that nothing in the act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder. This section was intended as specific recognition of the need to permit disclosure under the Freedom of Information Act.

The compromise amendment would add an additional condition of disclosure to the House bill which prohibits disclosure without written request of an individual unless disclosure of the record would be pursuant to Section 552 of the Freedom of Information Act. This compromise is designed to preserve the status quo as interpreted by the courts regarding the disclosure of personal information under that section.

A related amendment taken from the Senate bill would prohibit any agency from relying upon any exemption contained in Section 552 to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

CIVIL REMEDIES

Under the House bill an individual would be permitted to seek an injunction against an agency only to produce his record upon a failure of an agency to comply with his request. An individual would be able to sue for damages only if an agency failed to maintain a record about him with such accuracy, relevance, timeliness and completeness as would be necessary to assure fairness and a determination about him, and consequently an adverse determination was made. A suit for damages would also be in order against an agency if it fails to comply with any other provision of this act in such a way to have an adverse effect on the individual.

Under the Senate bill injunctive relief would be available to an individual to enforce any right granted to him. And an individual would be permitted to sue for damages for any action or omission of an officer or employee of the government who violates a provision of the act.

The standard for recovery of damages under the House bill would have rested on the determination by a court that the agency acted in a manner which was willful, arbitrary, or capricious. The Senate bill would have permitted recovery against an agency on a finding that the agency was negligent in handling his records.

These amendments represent a compromise between the two positions, permitting an individual to seek injunctive relief to correct or amend a record maintained by an agency. In a suit for damages, the amendment reflects a belief that a finding of willful, arbitrary, or capricious action is too harsh a standard of proof for an individual to exercise the rights granted by this legislation. Thus the standard for recovery of damages was reduced to "willful or intentional" action by an agency. On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed as only somewhat greater than gross negligence.

Both the House and Senate bills provided for an individual to recover reasonable attorney fees and costs of litigation. The compromise amendments adopt the standard of the House bill permitting the court to award attorney fees and reasonable costs to an individual where the complainant has substantially prevailed, in an injunctive action. Fees would be required to be paid with any award of damages.

ACCESS AND CHALLENGE TO RECORDS

The House bill would apply a standard of promptness to agency considerations of requests for access to records and requests to challenge or correct those records. In addition, it allows the individual to request a review of a refusal to correct a record by the agency official named in its public notice of information systems.

The Senate bill requires the agency to make a determination with respect to an individual's request for a record change within 60 days of the request and to permit him a hearing within 30 days of a request for one, with extension for good cause permitted. The individual would have the option of a formal or informal hearing procedure within the agency upon a refusal of a request to correct or amend a record. The compromise amendment would require the agency to respond within 10 working days to acknowledge an individual's request to amend a record. Following acknowledgement, the agency must promptly correct the information which the individual believes is not accurate, relevant, timely or complete or inform the individual of its refusal.

If the individual disagrees with the refusal of the agency to amend his record, the agency shall conduct a review of that refusal within 30 working days, provided that an extension may be obtained for good cause. We expect that agency heads will conduct these reviews themselves or assign officers of the rank of Deputy Assistant Secretary or above to review them.

The House bill would not have permitted a Federal District Court to review de novo an agency's refusal to amend a record. The compromise adopts the Senate provision which would require a de novo review of such refusal and to order a correction where merited. Finally, the compromise requires that in any disclosure of information subject to disagreement that the agency include with the disclosure a notation of any dispute over the information or a copy of any statement submitted by the individual stating his reasons for disagreement with the information.

ACCOUNTING FOR DISCLOSURES

Section c of the House bill requires an agency to inform any person or another agency about a correction or notation of dispute regarding a record that has been disclosed to that person or agency within two years before making the correction or notation. It would not apply if no accounting of the disclosure had been required. No such limitation was placed upon accounting for disclosures in the Senate bill and the compromise measure would require any person or agency receiving the record at any time before a notation or dispute is made to be notified if an accounting of the disclosures were made.

The House bill requires an agency to maintain an accounting for disclosures for only five years. The Senate bill places no limitation on the length of time

for maintaining such disclosures. The compromise amendment would require maintaining of the disclosure for five years or the life of the record, whichever is longer.

LIMITATIONS ON THE TYPES OF INFORMATION COLLECTED AND THE USE OF THIRD PARTY INFORMATION

The Senate bill requires Federal agencies to maintain only such information about an individual as is relevant and necessary to accomplish a statutory purpose of the agency. The House bill did not address this issue. The compromise amendment modifies the Senate provision to permit the collection of information which would be required to accomplish not only a purpose set out by a statute but also a purpose outlined by a Presidential Executive Order.

The provision is included to limit the collection of extraneous information by Federal agencies. It requires that a conscious decision be made that the information is required to meet the needs of an agency as dictated by a statute. Agencies should formulate as precisely as possible the policy objectives to be served by a data gathering activity before it is undertaken. It is hoped that multiple requests for information will be reduced and that agencies will collect no more sensitive personal information than is necessary.

The Senate bill also requires agencies to collect information to the greatest extent practicable directly from the subject when that information could result in an adverse determination about an individual's rights and benefits and privileges under a Federal program. The House bill had no provision, but the compromise amendment accepts the Senate language. This section is designed to discourage the collection of personal information from third party sources and therefore to encourage the accuracy of Federal data gathering. It supports the principle that an individual should to the greatest extent possible be in control of information about him which is given to the government. This may not be practical in all cases for financial or logistical reasons or because of other statutory requirements. However, it is a principle designed to insure fairness in information collection which should be instituted wherever possible.

ARCHIVAL RECORDS

The House bill provides that records accepted by the Administrator of General Services for temporary storage and servicing shall be considered for purposes of this act, to be maintained by the agency which deposits the records. Records transferred to the National Archives after the effective date of this Act for purposes of historical preservation are considered to be maintained by the Archives and are subject only to limited provisions of the Act. Records transferred to the National Archives before the effective date of this Act are not subject to the provisions of this Act.

The Senate bill provides that records accepted by the Administrator of General Services for temporary storage and servicing shall be considered, for purposes of this Act, to be maintained by the agency which deposits the records. All records transferred to the National Archives for purposes of historical preservation are considered to be maintained by the Archives and are subject only to those provisions of this Act requiring annual public notice of the existence and character of the information systems maintained by the Archives, establishment of appropriate safeguards to insure the security and integrity of preserved personal information, and promulgation and implementation of rules to insure the effective enforcement of those safeguards.

The compromise amendment subjects records transferred to the National Archives for historical preservation to a modified requirement for annual public notice. It is intended that the notice provision not be applied separately and specifically to each of the many thousands of separate systems of records transferred to the Archives prior to the effective date of this Act, but rather that a more general description be provided which pertains to meaningful groupings of record systems. However, record systems transferred to the Archives after the effective date of this Act are individually subject to the specific notice provisions. This coverage is intended to support and encourage improvements in the organization and cataloging of records maintained by the Archives, both to make authorized access to such records simpler and to insure broader application to Archival records of safeguards for data security and confidentiality.

MORATORIUM ON THE USE OF THE SOCIAL SECURITY ACCOUNT NUMBER

The House bill provides that a Federal agency, or a State or local government acting in compliance with Federal law or a federally assisted program, is prohibited from denying to individuals rights, benefits or privileges by reason of refusal to disclose the social security account number. Any such governmental agency is further prohibited from utilizing the social security account number for purposes apart from verification of individual identity except where another purpose is specifically authorized by law. Exempt from these prohibitions are systems of records in existence and operating prior to January 1, 1975. Exemption is further granted where disclosure of a social security account number is required by Federal law.

The Senate bill provides that a Federal agency, or a State or local government, is prohibited from denying to individuals rights, benefits or privileges by reason of refusal to disclose the social security account number. Persons engaged in the business of commercial transactions or activities are prohibited from discriminating against any individual in the course of such activities by reason of refusal to disclose the social security account number. Exempt from these prohibitions are systems of records in existence and operating prior to January 1, 1975. Also exempt are disclosures of the social security account number required by Federal law. This section further provides that any Federal, State or local government agency or any person who requests an individual to disclose his social security number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

The compromise amendment changes the House language by broadening the coverage of State and local governments so as to prohibit any new activity by such a government that would condition a right benefit or privilege upon an individual's disclosure of his social security account number.

To clarify the intent of the Senate and House, the grandfather clause of this section was re-stated to exempt only those governmental uses of the social security account number continuing from before January 1, 1975, pursuant to a prior law or regulation that, for purposes of verifying identity, required individuals to disclose their social security account number as a condition for exercising a right, benefit, or privilege. Thus, for illustration, after January 1, 1975, it will be unlawful to commence operation of a State or local government procedure that requires individuals to disclose their social security account number in order to register a motor vehicle, obtain a driver's license or other permit, or exercise the right to vote in an election. The House section was amended to include the Senate provision for informing an individual requested to disclose his social security account number of the nature, authority and purpose of the request. This provision is intended to permit an individual to make an informed decision whether or not to disclose the social security account number, and it is intended to bring recognition to, and discourage, unnecessary or improper uses of that number.

MAILING LISTS

The Senate bill prohibits the sale or rental of an individual's name and address by a Federal agency unless such action is specifically authorized by law. This section further provides that upon written request of any individual any person engaged in interstate commerce who maintains a mailing list shall remove the individual's name and address from such list.

The compromise amendment accepts the Senate prohibition of the sale or rental of mailing lists by Federal agencies. Names and addresses associated with other personal information obtained by Federal agencies pursuant to statute or executive order, or by unauthorized means, are thus not permitted to be sold or rented to the public. Public disclosure of mailing lists by authority of Section 552(b), the Freedom of Information Act, or by authority of other Federal law, is not prohibited. Public disclosure would be permitted in certain other circumstances where the agency determines that the potential for adverse effects from such disclosure on the privacy or other rights of persons on a mailing list are inconsequential and that the benefits likely to accrue to such persons and to the general public are clear and significant. In this regard, a directive from the Office of Management and Budget forbidding disclosure by Federal agencies of a person's name absent his specific consent would be relevant to the intent of this subsection.

RULEMAKING PROCEDURES FOR MAKING EXEMPTIONS

To obtain an exemption from certain provisions of this Act under the House bill, agencies entitled to those exemptions would be required to public notice of the proposed exemptions in the Federal Register pursuant to Section 553 of the Administrative Procedures Act permitting comments to be submitted in writing for inclusion in the Record with such exemptions.

The Senate bill applied a much more stringent standard and would have required agencies to hold adjudicatory hearings as provided in APA Sections 556 and 557. The compromise agreement would no longer require full adjudicatory proceeding by any agency seeking an exemption permitted under the act. However, agencies would still be required to publish notice of a proposed rulemaking in the Federal Register and could not waive the 30 day period for such publication. In addition it is specifically provided in this act that agencies obtaining such exemptions state the reasons why the system of records is to be exempted. Should objection be filed with the Commission to any rulemaking exemption, it is expected that the agency would respond specifically to each objection in setting forth its reason in support of the exemption.

DUTIES OF THE OFFICE OF MANAGEMENT AND BUDGET

Under the Senate bill the Privacy Protection Commission was directed to develop model guidelines and conduct certain oversight of the implementation of this Act to Federal agencies. Since the compromise amendment would change the scope of authority of the commission, it was felt there remained a need for an agency within the government to develop guidelines and regulations for agencies to use in implementing the provisions of the Act and to provide continuing assistance to and oversight of the implementation of the provisions of this Act by the agencies.

This function has been assigned to the Office of Management and Budget.

REPORTS ON NEW SYSTEMS

Under the Senate bill the Privacy Protection Commission was to have a central role in evaluating proposals to establish or alter new systems of information in the Federal government. If the commission had determined that such a proposal was not in compliance with the standards established by the Senate bill the agency which prepared the report could not proceed to establish or modify an information system for 60 days in order to give the Congress and the President an opportunity to review that report and the commission's recommendations.

The compromise amendment still would require that agencies provide adequate advance notice to the Congress and to the Office of Management and Budget of any proposal to establish or alter a system of records in order to permit an evaluation of the privacy impact of that proposal. In addition to the privacy impact, consideration should be given to the effect the proposal may have on our Federal system and on the separation of powers between the three branches of government. These concerns are expressed in connection with recent proposals by the General Services Administration and Department of Agriculture to establish a giant data facility for the storing and sharing of information between those and perhaps other departments. The language in the Senate report on pages 64–66 reflects the concern attached to the inclusion of this language in S. 3418.

The acceptance of the compromise amendment does not question the motivation or need for improving the Federal government's data gathering and handling capabilities. It does express a concern, however, that the office charged with central management and oversight of Federal activities and the Congress have an opportunity to examine the impact of new or altered data systems on our citizens, the provisions for confidentiality and security in those systems and the extent to which the creation of the system will alter or change interagency or intergovernmental relationships related to information programs.

GOVERNMENT CONTRACTS

The Senate bill would have extended its provisions outside the Federal government only to those contractors, grantees or participants in agreements with the Federal government, where the purpose of the contract, grant or agreement was to establish or alter an information system. It addressed a concern over the policy governing the sharing of Federal criminal history information with

State and local government law enforcement agencies and for the amount of money which has been spent through the Law Enforcement Assistance Administration for the purchase of State and local government criminal information systems.

The compromise amendment would now permit Federal law enforcement agencies to determine to what extent their information systems would be covered by the Act and to what extent they will extend that coverage to those with which they share that information or resources.

At the same time it is recognized that many Federal agencies contract for the operation of systems of records on behalf of the agency in order to accomplish an agency function. It was provided therefore that such contracts if agreed to on or after the effective date of this legislation shall provide that those contractors and any employees of those contractors shall be considered to be employees of an agency and subject to the provisions of the legislation.

DEFINITION OF RECORD

The definition of the term "Record" as provided in the House bill has been expanded to assure the intent that a record can include as little as one descriptive item about an individual and that such records may incorporate but not be limited to information about an individual's education, financial transactions, medical history, criminal or employment records, and that they may contain his name, or the identifying number, symbol, or other identifying particularly assigned to the individual, such as a finger or voice print or a photograph. The amended definition was adopted to more closely reflect the definition of "personal information" as used in the Senate bill.

DEFINITION OF THE TERM AGENCY

Some questions have been raised regarding the applicability of H.R. 16373 and S. 3418 to the U.S. Postal Service, the Postal Rate Commission and similarly related entities.

H.R. 16373 defines "agency" to mean an agency as defined in Section 552(e) of Title V. S. 3418 defines the term "Federal agency" to mean any department, agency, instrumentality, or establishment in the Executive Branch of the Government of the United States and includes any officer or employee thereof.

A compromise agreement adopts the definition by reference to section 552(e) as provided in H.R. 16373. It is the intention of the House and Senate that the Federal Privacy Act clearly apply to the Postal Service, the Postal Rate Commission, and government corporations or government controlled corporations now in existence or which may be created in the future as provided in Public Law 93–502, the amendments to the Freedom of Information Act.

While Section 410(a) of Title 39 of the U.S. Code exempts the Postal Service and Postal Rate Commission from legislation generally applicable to Federal agencies, barring a clear expression of Congressional intent to the contrary, is the considered intent of the committees which consider this legislation that it should apply to the Postal Service and Postal Rate Commission, notwithstanding the operation of Title 39 Section 14(a) of the United States Code.

Mr. ERVIN. Mr. President, I have also prepared a statement giving credit to members of the Government Operations Committee, and another statement giving credit to members of the Subcommittee on Constitutional Rights, which worked on privacy matters for many years, commending them for their work.

I would like to ask unanimous consent these be printed in the RECORD at this point.

There being no objection, the statements were ordered to be printed in the RECORD, as follows:

STATEMENT TO MEMBERS OF THE GOVERNMENT OPERATIONS COMMITTEE

Mr. President, S. 3418 represents the culmination of many months of work by the Committee on Government Operations to fashion legislation that will guarantee the rights of all Americans with respect to the gathering, use, and disclosure of information about them by the Federal Government.

Again, I want to express my gratitude to two members of this committee who have helped make this legislation possible, Senator Percy from Illinois, the ranking minority member, and Senator Muskie from Maine, the chairman of the Subcommittee on Intergovernmental Relations.

Their efforts, and that of their staffs have been indispensable in helping to reach the compromise reflected in the amendments adopted by the Senate today.

Great credit also is due to Senator Ribicoff, Senator Javits and the other cosponsors of this legislation as well as to all the members of the Committee on Government Operations. Without their many valuable contributions, we would have been unable to develop the sensible bill that the committee reported unanimously to the Senate.

Finally, the Committee wishes to express appreciation for the valuable time and effort devoted to the drafting of this legislation by Mr. Bill Ticer, in the office of the Senate Legislative Counsel.

Mr. President, I am pleased to note that the compromise which has been reached between the Senate and the House on this privacy legislation will provide for the establishment of a Privacy Protection Study Commission. While the scope of the commission's authority is not as broad as we had sought in the Senate bill, it should serve as an important function in providing the President and the Congress with the kind and caliber of information about problems related to privacy in the public and private sectors which are needed to make informed decisions.

I believe that this bill also strengthens the ability of the individual to enforce the rights granted to him under this act from the provisions which were contained in the House measure.

Finally the compromise bill contains the minimum recommendations made for protecting privacy and for establishing rules of due process for the Government's use of computer technology for personal data systems.

It is in keeping with the recommendation of the Committee on Government Operations which stated the purpose of the Senate bill is to:

Promote government respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerizing, collection, management, use and disclosure of personal information about individuals.

It is to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal government and with respect to all of its other manual or mechanized files.

It is designed to prevent the kind of illegal, unwise, over-broad, investigation and record surveillance of law-abiding citizens which has resulted in recent years from actions of some over-zealous investigators, from the curiosity of some government administrators, and from the wrongful disclosure and use of personal files held by Federal agencies.

It is to prevent the secret gathering of information or the creation of secret information systems or data banks on Americans by employees of the departments and agencies of the Executive branch.

It is designed to set in motion a long-overdue evaluation of the needs of the Federal government to acquire and retain personal information on Americans, by requiring stricter review within agencies or criteria for collection and retention of such information.

It is also to promote observance of valued principles of fairness and individual privacy by those who develop, operate and administer other major institutional and organizational data banks of government and society.

While this is a momentous day for the Senate, it's work in the filed of privacy is not completed with the adoption of this legislation. It will require aggressive oversight by the Committee on Government Operations, and I would hope that Senator Muskie through his Subcommittee on Intergovernmental Relations, and that Senator Percy, as the ranking minority member of the Committee on Government Operations, will continue to exercise their leadership in this regard.

STATEMENT TO MEMBERS OF THE SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

Mr. ERVIN. Mr. President, when the Senate approved S. 3418 in November, I paid tribute to the contributions of the members and the staff of the Government Operations Committee and to the staffs of the members of the Committee who

had worked on the bill. I wish to acknowledge also the valuable contributions of the Committee's special consultant, Professor Alan F. Westin of Columbia University whose testimony in June and expert counsel through the summer provided the basis for policy judgments and for detailed amendments of the bill in order that a workable proposal could be reported to the Senate. Professor Christopher Pyle of the John Jay College of Criminal Justice in New York, also rendered valuable assistance to the Committee, as he has during his service as a consultant of the Constitutional Rights Subcommittee.

Much credit is also due to Lawrence Baskir, former chief counsel of the Constitutional Rights Subcommittee, Mark Gitenstein, present chief Counsel of the Subcommittee, Irene Margolis, Dorothy Glauzer and the rest of the Subcommittee staff who helped immeasurably in the development of the bill and report during the joint hearings and study.

Furthermore, no person who has walked on Capitol Hill merits greater commendation in this connection than Marcia MacNaughton, who served for a substantial time on the staff of the Subcommittee on Constitutional Rights and made herself most knowledgeable in respect to privacy and the threats to it. During past months she left the academic world temporarily to aid the Senate Committee on Government Operations in the drafting of S. 3418.

I believe the comprehensive hearings and studies of the Constitutional Rights Subcommittee have helped to provide the Congress with an excellent basis for this and other needed legislation in years to come. I hope the many published volumes of the result of the Subcommittee's work on privacy, computers and data banks will aid those working on this subject in the future. The members who serve on that Subcommittee have made many contributions to the protection of privacy by their sponsorship of legislation and their support and participation of the investigations and reports which were needed to draft legislation. They have also provided the Executive Branch with the background and information for reports and action to protect privacy and I hope officials in all federal departments and agencies will continue to take advantage of this research and this documentation of public concern over governmental incursion on individual freedoms.

Since the Senate and the House passed their respective privacy bills, Jim Davidson has labored tirelessly to reconcile their varying provisions and thus make the enactment of legislation to protect the rights of privacy of Americans possible. I will always be grateful to him for his most helpful assistance to me.

Mr. ERVIN. Mr. President, I would urge all Members of the Senate to support these amendmetns with my assurance that I have been informed by the House that the House will immediately take them and send the bill to the White House and we will have, for the first time in the history of our Nation, some effective privacy legislation.

Mr. PERCY. Mr. President, the compromise privacy bill we bring before the Senate today is a remarkable achievement. It marks the culmination of more than 10 years of concern and attention by the Congress to the fundamental issue of personal privacy. It represents the continuing efforts by the distinguished senior Senator from North Carolina (Mr. Ervin) to cultivate that concern and I believe this legislation is a fine tribute to Senator Ervin's work.

I would like to strongly commend the staff of the Government Operations Committee in their efforts to produce a compromise with the House. Their diligent efforts have been quite crucial to the successful resolution of extremely difficult policy differences. In this regard, I would like to give a special commendation and extend my appreciation to Mr. Bill Ticer, office of the Senate Legislative Counsel, for his dedicated assistance to the committee staff during the past 6 months. I understand that his participation was of immense value in clarifying difficult portions of the legislation.

I also commend Congressman Moorhead of Pennsylvania, Congressman Erlenborn, and Congressman Goldwater for their diligent efforts in connection with this legislation.

I am pleased to note that the compromise which has been reached does include a provision for a 2-year Privacy Protection Study Commission. While this Commission does not retain some of the enforcement powers afforded to it in the Senate-passed bill, S. 3418, I believe that it is certainly equipped to perform the functions intended by the Senate. The Commission will be responsible for assembling experts in the fields of computer science, law, social sciences, business, and Government to study and recommend solutions to privacy problems not adequately addressed by this bill. I believe that the Commission will serve to keep focused attention on this important issue of public policy so that Federal agencies, State and local governments, and private organizations will continue to implement the basic principles of fair treatment for personal data contained in this bill.

I am pleased that the compromise bill contains the provision, introduced by Senator Goldwater and myself, to limit abuses of the social security number. I look forward to a more final solution to the problems associated with this number, which is widely used as a universal identifier in this country. The Privacy Protection Study Commission will study the problem and bring back to the Congress policy recommendations on this matter.

Finally, I am pleased that Congress has acted with authority to establish, across the board in the Federal Government, fundamental protections of personal privacy. The challenge now rests with the Federal agencies to adopt regulations and implement procedures to carry out the intent of this statute. We intend to work with the agencies and we hope that they will cooperate fully, in return, with the Government Operations Committees of both Houses, in their oversight capacity, and with the Privacy Protection Study Commission, in its study capacity.

Mr. MUSKIE. Mr. President, this is a momentous day for the Senate and for every citizen of this country on whom the Government maintains a record.

The compromise agreement which has been worked out between the Senate and the House under the able leadership of the chairman of the Committee on Government Operations, Mr. Ervin, represents the first major assault on the invasion of privacy in recent decades.

Mr. President, I would like to note the outstanding work in the development of this bill by Mr. James H. Davidson, of the staff of my Subcommittee on Intergovernmental Relations, who has spent countless hours working on this legislation.

The passage of this legislation will rightfully earn for this Congress the reputation as the Privacy Congress.

While the courts have begun to recognize the capacity and the practices of the Government to invade the privacy of its citizens, it is the responsibility of the Congress to develop the legislative protection against those invasions.

The Federal Privacy Act draws upon the constitutional and judicial recognition accorded to the right of privacy and translates it into a system of procedural and substantive safeguards against obtrusive Government information-gathering practices.

Until now we have allowed technological advances in Federal record-keeping to outpace our efforts to control and safeguard the information we have collected. This act would restore balance against those advances by adding new protections for every citizen.

I am pleased to note that this act has developed an important balance between the rights of privacy of each of our citizens and the public need for disclosure of Government materials under the Freedom of Information Act.

Mr. President, this legislation incorporates fundamental rights of fair information practices into Federal information systems. It is an important beginning. And I hope to be able to follow the implementation of this act in the next Congress through the work of my Subcommittee on Intergovernmental Relations.

Mr. BROCK. Will the Senator yield?

Mr. ERVIN. I yield to the Senator from Tennessee.

Mr. BROCK. Mr. President, may I take a moment to express my gratitude to the Senator from North Carolina for his leadership in a matter in which I have had, as so many others have had, a great, continuing, and growing concern. The privacy bill is a much-needed piece of reform legislation which I am proud to have sponsored.

There is no question about the abuse of personal privacy in this country, and it is growing at a geometric rate each year. I understand, for example, that it is presently possible to have every telephone in America bugged.

Privacy is not a privilege, it is a basic right, a fundamental freedom which is deeply rooted in our American heritage. It is the ability to be secure in our homes, persons, and papers. We simply must take firm and specific action to protect the people of this Nation from the erosion of their personal liberties.

This bill, which addresses itself to the use and abuse of Federal data banks, establishes several basic standards. First, only relevant personal information can be collected, and the individual must be informed as to which data is required, which is voluntary, why it is needed, and under which authority. Second, only timely data may be maintained and disseminated, and access to, and security of, the data must be regulated. Additionally, the nature of all data banks must be announced. Individuals will have access to inspect their records and must be told the source of the data and how it is used. Finally, information challenged by an individual must be reinvestigated and, where proper, modified or corrected.

I personally want to express my great debt to the Senator from North Carolina for his efforts to remedy this problem.

We did have differences with the House, but the compromise is an effort to deal with those differences in a very frank and very healthy way.

I appreciate the result of the labors of the gentleman and I want him to know it.

Mr. ERVIN. I thank my friend from Tennessee and want to commend him for the work he did in the Government Operations Committee in this legislation.

Mr. President, I ask for the yeas and nays on the motion.

The PRESIDING OFFICER. Is there a sufficient second? There is a sufficient second.

The yeas and nays were ordered.

Mr. ERVIN. I yield the floor.

Mr. HRUSKA. Mr. President.

The PRESIDING OFFICER. The Senator from Nebraska.

Mr. HRUSKA. Mr. President, I yield to the Senator from West Virginia, reserving my right to the floor, for a brief statement.

* * * * * * *

The Senate continued with the consideration of the message from the House of Representatives on the bill (S. 3418) to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes.

The PRESIDING OFFICER. The Senator from Nebraska.

Mr. HRUSKA. Mr. President, I rise to suggest that the consideration of the instant bill, S. 3418, pursuant to the motion of the Senator from North Carolina, is not exactly in keeping with the better traditions of this body regarding consideration of legislation of this gravity.

I am not going to take very long, but I would like to recite briefly the chronology of this legislation and what we are doing here today.

Last month, Mr. President, S. 3418 was approved by this body and sent to the other body. The bill, incidentally, as passed by the Senate, was about 40 printed pages in length.

The House also passed a measure, at approximately the same time, H.R. 16373, which dealt with the question of privacy of individuals' records. While many provisions of the House and Senate bill were similar, the Senate version contained provisions establishing a privacy commission, with far reaching powers, and providing extensive coverage of law enforcement records, features not found in the House bill.

The other body took the Senate bill S. 3418, and, upon consideration thereof, voted to strike all but the enacting clause and insert entirely in place therein the text of H.R. 16373, which consisted of approximately 20 printed pages. Apparently, the members of the Senate Government Operations Committee were displeased with the House version. There was contact established between the staff of the Government Operations Committee of the Senate and the staff of the Government Operations Committee of the House. There emanated therefrom, Mr. President, the text and the substance of the motion now pending by way of an amendment to the House bill, which I understand was completed yesterday.

This text, Mr. President, was submitted to my office less than 24 hours ago. It consists of approximately 40 pages of typewritten material. It is in many respects from the bill as passed by the Senate in the original instance. And it is different than the text of the bill that was approved by the other body.

In addition to that text, I was furnished by the very courteous and distinguished Senator from North Carolina with a copy of his remarks, consisting of an analysis of House and Senate compromise amendments to the Federal Privacy Act.

Let me suggest, Mr. President, that this occurred about 24 hours ago. I believe I received these remarks probably at 4 o'clock yesterday afternoon and the actual text of the amendment shortly after 6 p.m.

We adjourned the Senate, Mr. President, at about 6:40 p.m. yesterday. We convened at 9:30, as I remember it. I have been in committee most of the day. I started my first committee meeting at 9:30 this morning.

I know all of my colleagues have been very busy in the later part of this session, in the closing hours of this session.

I make no apology for the fact that I did not have time to read and to study this bill, nor the remarks of the Senator from North Carolina. I did impose upon my staff for the consumption on their part of a little midnight oil. I find, Mr. President, it is not quite as easy to explain the lack of difference between the House bill and the compromise bill as we might imagine.

There are some things that are of real substance. There are some items that are of very substantial difference; and, in my judgment, some items, on the basis of this staff analysis, that would bear close study and scrutiny, and which should receive a little more deliberate treatment than a mere consideration of the motion of amendment as proposed, and which we are considering now.

Let me suggest, Mr. President, first of all there is the suggestion, and there is the representation made, that the law enforcement files are exempted. Of course, that was one of our original objections to the bill as approved by the Senate. When I say "our" I mean those who are interested with me in the preservation of the integrity of law enforcement files, particularly the investigatory files, and to prevent a compromise thereof.

As I suggested at that time, the area of law enforcement files is of such complexity that it should not be dealt with on the same terms as civil records. I believe it can be readily understood that criminal justice or law enforcement information gives rise to problems requiring treatment different from that of information used to carry out the social health, or money benefit programs in which the Government may be involved. Law enforcement records should be treated in separate legislation.

The Senate Constitutional Rights Subcommittee presently has such legislation before it, S. 2963 and S. 2964. Many hours of hearings and research have gone into perfecting the provisions of this legislation in order to strike a proper and equitable balance between the individual's rights to privacy and society's interest in receiving good and effective law enforcement.

This legislation, represented by S. 2963 and S. 2964, is well along and near resolution. It is expected that similar legislation will be reported to the Senate floor early next year. It is my understanding that the Members in the House similarly expect to act on legislation dealing with law enforcement files early in the next Congress. It is further my understanding that this was the reason that H.R. 16373 contained an exemption from most of its provisions for criminal law enforcement files and records, an exemption which I found acceptable.

The staff compromise we have before us in the form of the amendment in question, however, narrows the law enforcement exemption, by making additional provisions of the bill applicable to law enforcement.

For example, the requirement that an accounting of all disclosures of a record be kept for a period of 5 years, "or for the life of the record, whichever is the longer" would now be applied to law enforcement files.

It should be noted that the statute of limitations for civil suits related to improperly disclosed records is only 2 years. The provision

that all future disclosures of the record be accompanied by notice of disputes as to its accuracy is also applied to law enforcement records.

Similarly, law enforcement would be covered by the requirement that proposed rulemaking hearings be held with respect to a statement of the routine uses to which records would be subject.

The expanded coverage of the law enforcement files is objectionable as a matter of principle, and may raise serious practical problems of which we may be unaware after only a brief study of the amendment.

Mr. PERCY. Would my distinguished colleague mind just a brief comment? If the distinguished Senator from Nebraska has finished the history of what happened on this legislation, I think for purposes of accuracy it would be well to make one insertion.

Mr. HRUSKA. I will yield briefly for that purpose. I do not want to detain the Senate too long. I shall cite one other example of detriment in the proposed amendment. Then I shall put the rest of this statement into the Record. If it is a brief comment, I will be happy to yield.

Mr. PERCY. I very much appreciate the deep interest that our distinguished colleague has taken in this legislation.

It would be, I believe, unfair to the Senate to assume, however, that what has resulted is a result only of staff discussions between the House and Senate. Obviously, on this legislation, as in most legislation, staff has done a great deal of work. But we cannot overlook the fact that Senator Ervin and myself, as the chairman and the ranking minority member of the Senate Government Operations Committee, and Congressman Moorhead of Pennsylvania, and Congressman Erlenborn, of Illinois, as the House Foreign Operations and Government Information Subcommittee chairman and the ranking minority member of the House Government Operations Committee, met together for a very extended session to discuss our respective bills.

We worked out compromises. We negotiated differences. We came to an accord, and we put the stamp of approval of two Senators and two Congressmen, representing the chairman and ranking members of the respective committees, before it was brought before the Senate today.

I believe that this one additional point would update and complete the historical account of this legislation up to this point.

I thank my distinguished colleague.

Mr. HRUSKA. I am happy to accept that supplement to the description of the history of this bill, Mr. President. It was not my intention to exclude from the consideration of the amendment before us the participation by members of the committee. But the bulk of the work, I am confident, was done by the staff. Many of the changes pertaining to law enforcement may have been inadvertently included with a full realization of their total effect.

Mr. President, I am just going to outline one other change. That has to do with the access to law enforcement records intelligence information by the privacy commission. The compromise with which we are now confronted would create a seven-member study commission with a broad mandate to examine privacy considerations as applied, Mr. President, to Federal, State, and private records.

The study commission would have full access to all information relating to the performance of their function, and it could issue sub-

penas as to enforce its request for information. I am concerned, Mr. President, that individual's rights may be offended by fishing expeditions by the commission into the raw background files maintained by the Government and into other particularly sensitive law enforcement and intelligence records.

I feel the compromise gives the commission too broad authority to examine Government records under the language in the bill.

I ask unanimous consent, Mr. President, that this memorandum, which was prepared by staff and from which I have quoted, and which I have checked with the text of the bill and its proposed compromise, be printed in the Record at this point.

There being no objection, the memorandum was ordered to be printed in the Record, as follows:

MEMORANDUM

The "final" staff compromise which is now before the Senate presents real problems for law enforcement generally.

Exemption of law enforcement files. H.R. 16373 contained an exemption from most of its provisions for criminal law enforcement files and records. It was acceptable in this regard. The staff compromise narrows the law enforcement exemption, thus making additional provisions of the bill applicable to law enforcement. For example, the requirement that an accounting of all disclosures of a record be kept for a period of five years "or the life of the record whichever is longer" would now be applied to law enforcement files. (Note that the statute of limitations for civil suits relating to improperly disclosed records is only two years). The provision that all future disclosures of the record be accompanied by notice of disputes as to its accuracy is also applied to law enforcement records. Compare p. 24 with page 9. Similarly, law enforcement would be covered by the requirement that proposed rule making hearings be held with respect to a statement of the "routine uses" to which such records would be subject, p. 17. The expanded coverage of law enforcement files is objectionable as a matter of principle and may raise serious practical problems.

New provisions concerning law enforcement. The staff compromise defines records as including not only collections of information about individuals but also an "item" of information about an individual. The intent of this change is not clear but it could be read so broadly as to include any single piece of paper bearing an individual's name within the meaning of record even though it may be filed as part of an investigatory file on a corporation or on some other individual. This would, among other things, require that annual notice of such "items" be published in the *Federal Register*. See § 3(a)(4) [p. 5]

The new definition of record also includes a reference to fingerprints, voice prints and photographs. The same reference is not included, however, in the description of those law enforcement files which may be exempted from provisions of the bill such as individual access to records or limitations on disclosure without the individual's consent. While it would be ludicrous to interpret the bill to require a fugitive's consent before his photograph is displayed on a wanted poster, the bill literally has this effect. Moreover, it may be read to permit individual access to photographs or voice prints in an investigatory file even though access to the file itself is not permitted by the bill. 3(a)(4) [p. 5]

"Routine" exchanges of information among government agencies—see 3(a)(7) [p. 6] 3 (b)(3) [p. 6]—are permitted by the bill so long as annual notice describing such routine exchanges is published. We were successful in obtaining a flower explanation of routine exchange in the House which would be helpful to law enforcement. The bill, however, has added a definition of "routine use" which may present problems for law enforcement. "Routine" use is defined as that which is compatible with the purpose for which the information was originally collected. There may be numerous exchanges of information with the FBI that are now undertaken by non-law enforcement agencies which would not fall within the scope of this definition, for example, information concerning possible civil disturbance activities. If such exchanges do not fall within

the definition of routine use then it would be necessary to secure the consent of the individual before furnishing it to the FBI or it would be necessary for the Director to make a written request for the information.

Since the information is of the sort normally brought to our attention only when it is voluntarily provided to us, the provision for requesting such records is virtually meaningless.

Among the new provisions added to the staff compromise is a requirement that before disseminating a record the agency must assure that the record is accurate, complete, timely and relevant. No standard is provided as to the proper application of these terms. The provision is applicable to law enforcement files as well as all other records. It would, of course, put the burden on the Identification Division to assure the completeness and relevance, as well as accuracy, of all rap sheets before dissemination. Moreover, it would appear to require that investigatory files be accurate, complete, timely and relevant before they are disseminated regardless of the purpose of the dissemination. Presumably this would even apply to old investigatory records made available pursuant to the historic records policy adopted under the Freedom of Information Act.—See § 3(e)(6) p. 16

Access to law enforcement records. The staff compromise would create a seven member study commission with a broad mandate to examine privacy considerations as applied to federal, state and private records. The study commission would have "full access to all information relating to the performance of their functions" and could issue subpoenas to enforce its requests for information. This could include requests for "raw files" and other sensitive law enforcement and intelligence records. The staff compromise, we feel, gives the Commission top broad authority to examine government records. [p. 38] § 5(e)(1)

Civil law enforcement problems. The bill requires that whenever an agency seeks information from an individual it must inform him of the source of its authority to seek the information, the purpose for which it is sought, routine uses that may be made of it, and the effects of not providing the information. Criminal law enforcement is exempt from these provisions but civil law enforcement is not. In certain cases such as civil frauds, civil rights investigations, antitrust investigations, etc. this may produce an inhibiting effect on a potential witness. (There is also incidental burden of including all of this information on all applicant forms as well.)

In a related vein, each agency is required to publish annually a description of its records systems. Except in the case of law enforcement, national defense, and similar files, a description of the "categories of sources" is to be included in the description. This too may present difficulties with respect to civil rights, fraud, and antitrust investigations where sources may require as much protection as they do in criminal cases.

An agency would be required to serve notice on an individual when a record pertaining to the individual is to be disclosed subject to "compulsory legal process." While law enforcement records would be exempt from this requirement, civil investigatory files would not be. Again this may present particular problems with respect to those civil actions which are quasi-criminal in nature. Moreover, it places an enormous burden on agencies and may, through motions to quash and similar interventions, seriously delay civil litigation.

Relationship to Freedom of Information Act. The Staff draft expressly provides that nothing in the Freedom of Information Act permits withholding a record from the subject of that record. This presents no serious problems since the bill itself permits withholding investigatory and similar files from the individual. The bill also provides, however, that disclosure is not permitted without an individual's consent unless disclosure would be required under FOI. Since the FOI Act itself authorizes the refusal of disclosure where this would constitute an "unwarranted invasion of privacy" the privacy bill's disclaimer of any intent to affect FOI is circular. In the face of the disclaimer, the government's efforts to mesh the two bills when faced with litigation over the nondisclosure of records to protect privacy may meet considerable difficulty.

Mr. HRUSKA. Mr. President, the motion before us and the amendment before us may be a good one. It may have merit. Maybe that would be the ultimate result of the action taken by the Senate.

As I indicated when S. 3418 was before us last month, Mr. President, I share the objective of my good friend from North Carolina to protect Americans in their right to privacy. The declared purposes of this bill are desirable and worthy. It is, Mr. President, only some of the specific features of the bill, which I have mentioned briefly, with which I have question.

I do not know how many copies of this 40-page typewritten manuscript which contains the compromise measure have been made, or how many are available. As I indicated, I did not get one in my office until 6:30 last night. I have not made inquiry as to its distribution. It just seems to me that notwithstanding the lateness of this session, this subject and this measure are entitled to a little more deliberate, proper, and complete consideration by the Senate. It is an important subject and I hope that in our rush to enact this legislation that we are not inadvertently including provisions that will trouble us later.

I have no disposition to get into the matter of proposing an amendment at this time. If I did, Mr. President, I would propose an amendment by way of a substitute to reinstate, a substitute for the Ervin amendment, by way of a substitute to that, the text of the bill as originally passed by the House, which was understandable, which had been closely studied; and with which we have had some familiarity. I shall not do that, because to do that at this late hour would be putting the Senate in the same position with regard to that substitute measure that it is placed in with regard to the principal amendment—to wit, we would not have that discretion and we would not have that amplification upon the content of the amendment, and that would not be fair.

So I submit again, Mr. President, that it is a mistake to proceed at this late hour with the consideration of the pending amendment. It is my hope that it will not be approved. If the amendment before us does not succeed, we will have before us the House version of the privacy bill which I find an extremely meritorous measure. It will readily achieve the objectives of the protection of privacy we seek and would receive my strong support.

The PRESIDING OFFICER. The question is on agreeing to the motion of the Senator from North Carolina. On this question the yeas and nays have been ordered, and the clerk will call the roll.

The legislative clerk called the roll.

Mr. ROBERT C. BYRD. I announce that the Senator from Texas (Mr. BENTSEN), the Senator from Nevada (Mr. BIBLE), the Senator from Alaska (Mr. GRAVEL), the Senator from Rhode Island (Mr. PASTORE), the Senator from California (Mr. CRANSTON), the Senator from Mississippi (Mr. EASTLAND), the Senator from Arkansas (Mr. FULBRIGHT), the Senator from Louisiana (Mr. JOHNSTON), the Senator from Arkansas (Mr. MCCLELLAN), the Senator from Connecticut (Mr. RIBICOFF), and the Senator from Georgia (Mr. TALMADGE) are necessarily absent.

I further announce that the Senator from Montana (Mr. MANSFIELD) is absent on official business.

I also announce that the Senator from Maine (Mr. HATHAWAY) is absent because of a death in the family.

I further announce that, if present and voting, the Senator from Rhode Island (Mr. PASTORE) would vote "yea."

Mr. GRIFFIN. I announce that the Senator from Oklahoma (Mr. BELLMON) and the Senator from Utah (Mr. BENNETT) are necessarily absent.

The result was announced—yeas 77, nays 8, as follows:

[No. 567 Leg.]

YEAS—77

Abourzek	Goldwater	Montoya
Allen	Griffin	Moss
Baker	Hansen	Muskie
Bartlett	Hart	Nelson
Bayh	Hartke	Nunn
Beall	Haskell	Packwood
Biden	Hatfield	Pearson
Brock	Helms	Pell
Brooke	Hollings	Percy
Buckley	Huddleston	Proxmire
Burdick	Hughes	Randolph
Byrd, Harry F., Jr.	Humphrey	Roth
Byrd, Robert C.	Inouye	Schweiker
Cannon	Jackson	Scott, Hugh
Case	Javits	Scott, William L.
Chiles	Kennedy	Sparkman
Church	Long	Stafford
Clark	Magnuson	Stennis
Cook	Mathias	Stevens
Dole	McClure	Stevenson
Domenici	McGee	Symington
Dominick	McGovern	Thurmond
Eagleton	McIntyre	Tunney
Ervin	Metcalf	Weicker
Fannin	Metzenbaum	Williams
Fong	Mondale	

NAYS—8

Aiken	Gurney	Tower
Cotton	Hruska	Young
Curtis	Taft	

NOT VOTING—15

Bellmon	Eastland	Mansfield
Bennett	Fulbright	McClellan
Bentsen	Gravel	Pastore
Bible	Hathaway	Ribicoff
Cranston	Johnston	Talmadge

So Mr. Ervin's motion to concur in the House amendment with amendments was agreed to.

Mr. ERVIN. Mr. President, I move to reconsider the vote by which the Senate amendments were agreed to.

Mr. CHURCH. Mr. President, I move to lay that motion on the table.

The motion to lay on the table was agreed to.

Mr. ROBERT C. BYRD. Mr. President, I ask unanimous consent that the Senator from Washington (Mr. JACKSON) may proceed for 1 minute.

The PRESIDING OFFICER. Without objection, it is so ordered.

[From the Congressional Record—Senate, Dec. 18, 1974]

SENATE CONSIDERS AND ADOPTS THREE TECHNICAL AMENDMENTS PASSED BY THE HOUSE WHICH FURTHER AMEND THE SENATE-HOUSE COMPROMISE AMENDMENTS TO S. 3418

Mr. ERVIN. Mr. President, I ask the Chair to lay before the Senate a message from the House of Representatives on S. 3418.

The Presiding Officer (Mr. NUNN) laid before the Senate the amendments of the House of Representatives to the amendments of the Senate to the amendments of the House to the bill (S. 3418) to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes as follows:

(1) Page 16, strike out lines 1 through 10, inclusive, and insert:

"(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

"(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

(2) Page 24, strike out all after line 10 over to and including line 24 on page 25, and insert:

"(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

"(1) maintained by the Central Intelligence Agency; or

"(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compelled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 552(c) of this title, the reasons why the system of records is to be exempted from a provision of this section."

(3) Page 42, strike out lines 11 through 21, and insert:

"(h)(1) Any member, officer, or employee of the Commission, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

"(2) Any person who knowingly and willfully requests or obtains any record concerning an individual from the Commission under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000."

Mr. ERVIN. Mr. President, the House amendments to the Senate amendments to the House amendments are merely technical in nature and there is no opposition to them, so far as I can find.

I would therefore move that the Senate concur in the House amendments to the Senate amendments to the House amendments.

The PRESIDING OFFICER. The question is on agreeing to the motion of the Senator from North Carolina (Mr. Ervin).

The motion was agreed to.

HOUSE ACTION

[From the Congressional Record—House, Nov. 20, 1974]

HOUSE CONSIDERS H.R. 16373

Mr. MURPHY of Illinois. Mr. Speaker, by direction of the Committee on Rules, I call up House Resolution 1419 and ask for its immediate consideration.

The Clerk read the resolution as follows:

H. RES. 1419

Resolved, That upon the adoption of this resolution it shall be in order to move that the House resolve itself into the Committee of the Whole House on the State of the Union for the consideration of the bill (H.R. 16373) to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies. After general debate, which shall be confined to the bill and shall continue not to exceed one hour, to be equally divided and controlled by the chairman and ranking minority member of the Committee on Government Operations, the bill shall be read for amendment under the five-minute rule. It shall be in order to consider the amendment in the nature of a substitute recommended by the Committee on Government Operations now printed in the bill as an original bill for the purpose of amendment under the five-minute rule. At the conclusion of such consideration, the Committee shall rise and report the bill to the House with such amendments as may have been adopted, and any Member may demand a separate vote in the House on any amendment adopted in the Committee of the Whole to the bill or to the committee amendment in the nature of a substitute. The previous question shall be considered as ordered on the bill and amendments thereto to final passage without intervening motion except one motion to recommit with or without instructions.

Mr. MURPHY of Illinois. Mr. Speaker, I yield 30 minutes to the minority, to the distinguished gentleman from Ohio (Mr. Latta), pending which I yield myself such time as I may consume.

(Mr. Murphy of Illinois asked and was given permission to revise and extend his remarks.)

Mr. MURPHY of Illinois. Mr. Speaker, House Resolution 1419 provides for an open rule with 1 hour of general debate on H.R. 16373, the Privacy Act of 1974.

House Resolution 1419 provides that it shall be in order to consider the amendment in the nature of a substitute recommended by the Committee on Government Operations now printed in the bill as an original bill for the purpose of amendment under the 5-minute rule.

H.R. 16373 permits an individual to have access to records containing personal information on him kept by Federal agencies for purposes of inspection, copying, supplementation and correction, with certain exceptions, including law enforcement and national security records.

H.R. 16373 also allows an individual to control the transfer of personal information about him from one Federal agency to another for nonroutine purposes by requiring his prior written consent.

H.R. 16373 also provides a civil remedy each loan involving energy-related products and services and a statement assessing the impact of each such loan on the availability of such products, services, or energy supplies for use in the United States.

Finally, I believe I should point out that this legislation specifies that until such time as the Trade Reform Act is approved by the Congress and signed into law by the President, no loan, guarantee, insurance, or credit shall be extended by the Bank to the Soviet Union.

Mr. Speaker, I urge adoption of the conference report.

* * * * * * *

Mr. DERWINSKI. Mr. Speaker, will the gentleman yield?

Mr. MURPHY of Illinois. I will be happy to yield to the gentleman from Illinois.

Mr. DERWINSKI. Mr. Speaker, I had a number of questions about this rule and the bill, but the gentleman from Illinois (Mr. Murphy) described it in such a truly effective fashion that I at this point do not have any questions.

I commend the gentleman for the scholarly presentation.

Mr. MURPHY of Illinois. I thank the gentleman for that comment.

Mr. Speaker, I yield to the gentleman from Ohio (Mr. Latta).

(Mr. Latta asked and was given permission to revise and extend his remarks.)

Mr. LATTA. Mr. Speaker, this rule, House Resolution 1419 provides for the consideration of H.R. 16373, the Privacy Act of 1974. There will be 1 hour of general debate on the bill and it will be open to all germane amendments. In order to preserve the normal amending process, the rule makes the committee substitute in order as an original bill for the purpose of amendment.

The general purpose of H.R. 16373 is to protect the privacy of individuals by regulating the Federal Government's collection and use of personal information.

The bill includes provisions to do the following things: (a) The bill permits an individual to have access to records containing personal information on him kept by Federal agencies for purpose of inspection and correction, with some exceptions, such as national security and law enforcement records. (b) The bill will make known to the American public the existence and characteristics of all personal information systems kept by every Federal agency. (c) The bill prohibits any Federal agency records from including information on political and religious beliefs unless authorized by law or the individual himself. (d) The bill provides a civil remedy by individuals who have been denied access to their records or whose records have been kept or used in violation of this act. The plaintiff may recover actual damages and costs and attorney's fees if the agency's violation was willful, arbitrary or capricious. (e) The bill provides that anyone who obtains a Federal record containing personal information by false pretenses is subject to a fine up to $5,000.

Mr. Speaker, I would like to point out that on October 9 the President sent a message up here in which he stated as follows:

H.R. 16373, the Privacy Act of 1974, has my enthusiastic support, except for the provisions which allow unlimited individual access to records vital to determining eligibility and promotion in the Federal service and access to classified information. I strongly urge floor amendments permitting workable exemptions to accommodate these situations.

The cost of implementing this bill is estimated to be between $200 million and $300 million a year, with a one-time "start up" cost of $100 million.

Mr. MURPHY of Illinois. Mr. Speaker, I have no further requests for time, and I move the previous question on the resolution.

The previous question was ordered.

The resolution was agreed to.

A motion to reconsider was laid on the table.

Ms. ABZUG. Mr. Speaker, I move that the House resolve itself into the Committee of the Whole House on the State of the Union for the consideration of the bill (H.R. 16373) to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies.

The SPEAKER. The question is on the motion offered by the gentlewoman from New York (Ms. Abzug).

The motion was agreed to.

IN THE COMMITTEE OF THE WHOLE

Accordingly the House resolved itself into the Committee of the Whole House on the State of the Union for the consideration of the bill, H.R. 16373, with Mr. Brademas in the chair.

The Clerk read the title of the bill.

By unanimous consent, the first reading of the bill was dispensed with.

The CHAIRMAN. Under the rule, the gentleman from California (Mr. Holifield) will be recognized for 30 minutes, and the gentleman from Illinois (Mr. Erlenborn) will be recognized for 30 minutes.

The Chair recognizes the gentleman from California (Mr. Holifield).

Mr. HOLIFIELD. Mr. Chairman, I yield 9 minutes to the gentleman from Pennsylvania (Mr. Moorhead).

(Mr. Moorhead of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, it is with a deep feeling of honor and pride that I present to the House of Representatives today H.R. 16373, "The Privacy Act of 1974."

Like the Freedom of Information Act, this bill is also totally bipartisan. It was approved by the Committee on Government Operations by a unanimous rollcall vote of 39 to 0. It has the enthusiastic support of President Ford except on one point which the House itself will resolve when an amendment is offered on the floor. More important, I sincerely believe such legislation has the widespread support of the American people. I believe they want us to act on this bill without delay.

It seems to me that the events of the past several years have a lesson in them. Americans want to see more credibility in Government, and they want to see the removal of any undue Government power which could be used to invade their personal privacy.

This landmark legislation, H.R. 16373, is a first step in that direction. It is in total harmony with the spirit of the Constitution. It gives individuals as a matter of right some meaningful control over how the Federal Government utilizes personal information about them.

H.R. 16373, when passed and signed by the President, will be the first comprehensive law dealing with the right of privacy of the individual citizen.

At the outset, I should state that this bill affects only personally identifiable files or systems of files held by the Federal Government. It does not seek to regulate those files maintained by State or local governments or by private entities.

Although this bill appears complicated on its face, it breaks down into four straightforward provisions: First, notice; second, access; third, regulation of disclosure, and fourth civil and criminal remedies.

NOTICE

Basically the bill provides that each and every system of records, as defined by the act, shall be made public by notice in the Federal Register. This notice shall list the essential characteristics of the system, the categories of persons to which it applies, its physical characteristics, the uses to which it is put, and the person responsible for its maintenance and operation.

ACCESS

Each individual shall be given access to his record within the system on his request, with the exception of files related to criminal investigations or national security. Along with access to the file, the individual concerned shall have the right to challenge inaccurate information and supplement the file to explain or contradict inaccuracies.

DISCLOSURE

Disclosure of the information by the agency holding the file shall be limited to those disclosures which are of the type previously announced in the Federal Register. Other disclosures of a "nonroutine nature" may be made only upon the prior written informed consent of the individual concerned.

REMEDIES

Civil damages are available to individuals who are injured by determinations made on the basis of inaccurate or incomplete records and criminal penalties are provided for illegal disclosure by Government employees, or fraudulent access by individuals.

I am going to say something very important now, especially in light of disclosures during the last week or so on the Federal Bureau of Investigation and the Internal Revenue Service. H.R. 16373 also prohibits the Government from keeping secret personal information sys-

tems and collecting records on political and religious beliefs. This proposed statute would thus provide greater safeguards for protecting the lawful exercise of first amendment rights.

The remainder of the provisions of the bill are designed to provide the legal teeth to enforce these rights and limitations. Special provision is made to protect America's legitimate and legally authorized interests in national security and law enforcement.

We have tried to tailor this bill so that it will protect individual rights and at the same time permit the Government to operate responsibly and perform its functions without unjustifiable impediments.

As a result, we think it will go a long way in restoring confidence by the American people that Government is indeed responsive and sensitive to individual rights. Simply put, this legislation will demonstrate that Congress is determined that Government will act as the servant of the people and not its master.

Under a key provision of this bill, no Federal agency shall disclose any personal information record to another agency or person unless this action is done by request of the individual or with his prior written consent.

An exception is permitted in the case of routine transfers, such as when the Social Security Administration instructs the Treasury to issue a benefit check.

Thus routine transfers of personal information will be permitted between agencies so that the regular business of Government can proceed without delay. Nonroutine transfers, however, are another matter. In those cases, the prior written consent of the individual will be required by law.

What is a nonroutine transfer? That is a transfer of personal information used for a different purpose than for which it was originally collected. This in itself is going to stop a lot of hanky-panky. It will make it legally impossible for the Federal Government in the future to put together anything resembling a "1984" personal dossier on a citizen.

It means interagency computer data banks will not be able to share personal information unless the data is truly a routine transfer where its general use has already been made known to the individual and his consent obtained.

The consent requirement and other provisions of the bill are backed up with criminal and civil penalties. This also will help protect Americans and at the same time give Government officials a good reason to say "no" to any improper requests from anyone for personal information on any other American.

This legislation also requires that Federal agencies, in making determinations on individuals, utilize records which are accurate, relevant, timely, and complete. This assures fairness to the individual and, in our view, is going to result in much better decisions by Government officials.

Senator Ervin has referred to the situation existing now as "the Government's voracious appetite for personal information about each of us."

His subcommittee reported that the Federal Government has at least 858 data banks of which 741 were computerized. Although 93 agencies did not report the number of records kept, those which did, reported a

total number of records kept as 1 billion, 245 million individual records for every man, woman, and child in America.

When such information is stored on tape it is easily transferred from one user to another.

The potential danger to individual freedom is so great that it is easy to understand why the concept of legislation to protect the privacy has support from a broad spectrum of political and philosophical beliefs.

I think the Members should be aware of the fact that in the event of the failure of Congress to act on this legislation, the President intends to issue an Executive order which would put a similar privacy system into effect. However, it would lack the necessary civil remedies and criminal penalties to provide our citizens with adequate redress. Besides, this task is a congressional responsibility and I think you will agree, we should face up to it.

On another matter, our subcommittee has received numerous phone calls from State tax commissioners asking whether their tax information transfer agreements with the U.S. Internal Revenue Service will be harmed by this bill. The answer is "no," because I am certain the Treasury Department will publish that type of activity as a "routine transfer" permitted under this bill and other statutes.

My colleagues, H.R. 16373 actually is the result of an awareness of the problems of invasion of privacy which began growing more than a decade ago when the House Committee on Government Operations started its initial investigations into this subject. Other committees also discovered what these problems are.

A lot of water has passed under the bridge since then. The Nation has survived numerous major and minor "floods." It is now time to build a strong dam to make certain we are not endangered again. I beseech you to support this bill and implement the Constitution, as we have a duty to do.

Mr. DENNIS. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from Indiana.

Mr. DENNIS. I thank the gentleman for yielding. With reference to the gentleman's statement that this would keep the Government from maintaining records as to political beliefs, would this bill prevent the Federal Bureau of Investigation from maintaining a list of Communist Party members or people who belong to organizations which are dedicated to the violent overthrow of the Government, or anything of that sort?

Mr. MOORHEAD of Pennsylvania. Lawful criminal investigations of that type would be exempt from the bill, but normal dissidents, exercising first amendment rights, would be covered.

Mr. DENNIS. If it hinged on the criminal field, it would come under the exemption which was referred to earlier?

Mr. MOORHEAD of Pennsylvania. The gentleman is correct.

Mr. DENNIS. And would the gentleman agree that if it dealt with individuals or organizations dedicated to the violent overthrow of the Government, that that would fall within the criminal exemption?

Mr. MOORHEAD of Pennsylvania. Anything that falls within the criminal exemption is taken care of. We have tried to prepare it very carefully.

Mr. DENNIS. Activity dedicated to violent overthrow of the Government would fall under criminal exemption, would the gentleman agree with me on that?

Mr. MOORHEAD of Pennsylvania. Yes. That is what I am saying.

Mr. DENNIS. I thank the gentleman.

Mr. HOLIFIELD. Mr. Chairman, I yield 5 minutes to the gentlewoman from New York (Ms. Abzug).

(Ms. Abzug asked and was given permission to revise and extend her remarks.)

Ms. ABZUG. Mr. Chairman, this is indeed a landmark piece of legislation. H.R. 16373 regulates the collection, maintenance, and use by Federal agencies of information pertaining to individuals. It is a very significant first step in an attempt to guarantee the right of privacy to all Americans. It is the product of many, many months of hard work, and of many bills that have been before the Congress which the committee has considered in great depth. Much credit is due to my colleague, Mr. Moorhead of Pennsylvania, the chairman of the Foreign Operations and Government Information Subcommittee, and to that subcommittee's staff members for the months of diligent effort in the drafting of this significant legislation. The bill which has been reported out of the committee is a good bill, but I believe it is a bill which requires some additions and changes to strengthen it. The amendments which I plan to offer today in connection with this bill are amendments which would have been brought before the full committee, but, in order to expedite the consideration and the bringing of the bill to the floor of the House, they were left for floor action. So, although I support the bill and, indeed, have been the author of one of the bills before the committee, along with the gentleman from New York (Mr. Koch) and the gentlemen from California (Mr. Goldwater) who also had bills which were considered by the committee, I feel that there have to be some improvements.

There are three basic weaknesses in the bill: the numerous and unjustified exemption provisions, the failure to provide either liquidated or punitive damages, and the lack of any administrative mechanism to oversee the implementation of the bill.

First, exemptions from the provisions of this bill or of any bill designed to protect individual rights of privacy can be justified only in the face of overwhelming societal interests. There are, at most, only three areas where societal interests can be paramount to the individual rights provided in this bill: First, where granting an individual access to his or her records would seriously damage national defense or foreign policy; Second, where such access would interfere with an active criminal prosecution; and Third, where records are required by law to be maintained for statistical research or reporting purposes and are not, in fact, used to make determinations about identifiable individuals.

It follows that exemptions should relate to the type of data sought to be protected from disclosure, not to the agency maintaining such records. For this reason, I will offer amendments to eliminate the general agency exemptions provided in the bill for the CIA and the Secret Service.

I will also support an amendment to provide for the assessment of punitive damages in cases of willful, arbitrary, or capricious viola-

tion of the bill and for actual damages in cases of negligent violations. These provisions were stricken in the full committee, and, as a result, an individual who may have suffered by violation of the act must now prove not only actual damages but that such damages were caused by willful, arbitrary, or capricious agency action. I believe that these two stricken-out provisions must be restored to the bill to provide, as the bill in the other body does, for actual damages to compensate for any violation of the act and for punitive damages to compensate for any willful, arbitrary, or capricious violation. If this is not done, there really is no adequate remedy at law.

I will also support an amendment which I brought in the committee to establish a Federal Privacy Commission. Without such a commission, we have no assurance that agencies will not be motivated by mere whim or convenience in divulging or withholding information.

We would be more than naive if we failed to recognize that individual Federal agencies cannot be expected to take an aggressive role in enforcing privacy legislation. Enforcement of the provisions of this bill will be secondary to each agency's legislative mandate and will, of necessity, cause additional expense and administrative inconvenience. Only by providing a separate administrative agency with authority for implementing this legislation and for coordinating the privacy programs of the various Federal agencies can we be assured of uniform, effective enforcement of the rights guaranteed by this bill.

I would hope that we will support this bill with the amendments proposed. I think that will be the beginning of an important first step in the protection of the right of privacy.

(Ms. Abzug asked and was given permission to revise and extend her remarks.)

Mr. ERLENBORN. Mr. Chairman, I yield myself 5 minutes.

(Mr. Erlenborn asked and was given permission to revise and extend his remarks.)

Mr. ERLENBORN. Mr. Chairman, I rise in support of the Privacy Act of 1974, H.R. 16373. I think it is rather fitting that this bill comes to the floor today on the same day that we considered a motion to override and have overridden the President's veto on the Freedom of Information Act.

The Subcommittee of Government Operations, known as Foreign Operations and Government Information, is the parent subcommittee of both bills, the Freedom of Information Act and now this new Privacy Act. It has been quite an effort to walk a tightrope in the one bill to provide the maximum access to information on the part of the public, and in the other bill to limit access to protect an individual privacy.

There has been a tendency, I think, to view these often as conflicting, but I think that we have successfully walked that tightrope and have, in both of these pieces of legislation, very important landmark legislation for open government, and yet the protection of individual rights.

The Privacy Act of 1974 does several things that I am sure will be delineated and explained by the several Members who will be engaged in debate. Generally it requires that when the Federal Government does maintain a system of records pertaining to individuals, it must identify publicly those systems of records. There will no longer be the ability within Government to maintain secret systems.

Not only in the past has this been done for any nefarious purpose, but the system of records may be instituted and maintained and the public just not know about it.

So that is the first thing that will be done: identify the systems of records and make public the fact that such records are being maintained.

Second, again a public record would be made of the purpose for which the system is being maintained. Then we would limit in the bill access to these records for those purposes so that information contained in those systems would be used only for those routine purposes, and unless the individual about whom the information related agreed to its use for other than routine purposes, it could not be so used.

It could be used then only for the routine purposes. This limits the purpose and the use of these information systems to the public purpose which has been made known, the purposes identified in the Federal Register.

Third, we provide for access by individuals to information in these record systems pertaining to himself or herself, so that a person about whom information has been collected will have an opportunity to get a copy of that information and to see if it is accurate and will have the procedure where he can request the amendment of the information to make it accurate and will have an opportunity if the information is misused under the terms of the act for recourse in a civil action through the courts.

In addition criminal penalties are provided for people within Government who violate the terms of the act in making information available that they should not, thereby invading the privacy of the individuals about whom the information is maintained and also criminal penalties for those who would seek and obtain illegally this information.

I think this is truly landmark legislation. It has been very difficult to draft because of the varying systems and the varying purposes for the systems within the Federal Government. We were of course, at times importuned to expand this to all record systems, not just of the Federal Government but of States and local governments and also in the private sector. I think if we had done so we would have bitten off more than we could chew.

I think we have here maybe a modest beginning in the field of privacy but we have an important piece of legislation affecting only Federal Government systems.

We generally exempt from the provisions of this bill the law enforcement proceedings, systems for the criminal justice system, and other committees of Congress will be turning and already have turned their attention to this criminal justice field.

There is one amendment that I hope will be adopted. Several will be offered and I will offer one amendment and I hope it will be adopted and I think it is crucial in making this a workable bill. The bill as it has been reported by the committee and is before us today will open up all preemployment and security clearance files retroactively as well as prospectively. Just think of this. In the past years there have been implied and expressed promises of confidentiality given to people who have been asked to make statements concerning the security clearance

investigation or preemployment investigation for those who would be employed by the Federal Government, appointed to Federal office, or Federal contractors engaged in defense work, let us say. These promises of confidentiality would be violated by this bill because the bill would mandate opening up these files so that the person about whom the investigation was conducted would have access to the files and find out who said what about them.

In the name of privacy we would be violating the privacy of those who have given such statements in the past. I think we have to strike a balance and see that we cannot violate the privacy of individuals by the very bill that is supposed to be the bill of rights for individual privacy.

The amendment I will offer was discussed in an editorial in the Washington Post this morning inaccurately. They say my amendment would close these preemployment and security files. It would not.

Mr. Chairman, the amendment that I will offer will make all of the information in these files available to the individual about whom the investigation has been conducted, except that information which would reveal the identity of a person who has under a promise of confidentiality given information contained in the file. Even the Washington Post editorial suggested that other legislation in the field of credit, the Fair Credit Reporting Act, had struck a good balance here by saying it is to protect only that information which would reveal a confidential source. They seem to think that was a good way of protecting both individuals' privacy. That is exactly what the amendment that I will offer will do. It will protect only those sources that have given information under a promise of confidentiality.

In addition, the Office of Management and Budget has assured me that regulations will be adopted in the future so that only in the most compelling circumstances will a promise of confidentiality be given. It will not be the customary thing to make these promises of confidentiality, so that most all of the information will be made available.

Mr. BROWN of Ohio. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I yield to the gentleman from Ohio.

Mr. BROWN of Ohio. For the purpose of making legislative history, I should like to ask about the impact of this legislation as it affects one aspect of the current law.

I currently represent an area which at one time was represented by one of our predecessors in the Congress, the illustrious Jackson Betts, who was very concerned about the confidentiality of the Bureau of Census information.

The CHAIRMAN. The time of the gentleman has expired.

Mr. ERLENBORN. I yield myself 2 additional minutes.

Mr. BROWN of Ohio. Mr. Chairman, the Bureau of the Census has a singular and highly commendable record of scrupulous protection of the confidentiality and privacy of census data about individuals and about businesses.

This is a matter of concern to every American, and the integrity of such information is essential to the public trust which is in turn essential to the accuracy of census findings.

These census findings provide the factual basis for: First, countless governmental and private decisions which profoundly affect the economy, second, equity and fairness in revenue sharing measures, and third, the determination of representation in the Congress.

The continuing confidentiality of such census information is mandated by statute—section 9 of title 13 of the United States Code—as affirmed by repeated Presidential proclamations.

It is true that neither the purpose nor effect of subsection (b) or (1) or of any other provisions of section 562a as set forth in this bill are to modify or relax in any way the safeguards of title 13?

Mr. ERLENBORN. Mr. Chairman, the answer to the gentleman's question is that this bill in no way would diminish the protection provided by law for census data.

Mr. BROWN of Ohio. I wonder if the gentleman would yield further so that I might receive the concurrence of the chairman of the subcommittee, the gentleman from Pennsylvania (Mr. Moorhead).

Mr. ERLENBORN. Mr. Chairman, I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. I agree with the remarks of the gentleman from Ohio and with the gentleman from Illinois.

Mr. DENNIS. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I yield to the gentleman from Indiana.

Mr. DENNIS. I would like to make reference to the question of criminal records, publication of criminal records, which are generally exempted from the bill, as I understand it.

The gentleman said a moment ago that those records are the subject of pending special legislation, and obviously those are very sensitive records and present a peculiar problem, and the subcommittee of the Committee on the Judiciary, chaired by the gentleman from California (Mr. Edwards) and of which the gentleman from California (Mr. Wiggins) is the ranking minority member, has special legislation on that subject now before it. That subcommittee is tied up in a meeting today on a very important matter that the members of the subcommittee could not avoid, and hence they are not on the floor; and they have asked me to bring the matter up and express the strong hope that the House adopt no amendment that would impinge on that situation and would include criminal records in this bill.

Mr. ERLENBORN. Mr. Chairman, I yield such time as he may consume to the ranking member of the Committee on Government Operations, the gentleman from New York (Mr. Horton).

(Mr. Horton asked and was given permission to revise and extend his remarks.)

Mr. HORTON. Mr. Chairman, I rise in support of H.R. 16373, the Privacy Act of 1974.

Having served as a member of the Special Subcommittee on Invasion of Privacy of the Committee on Government Operations some 10 years ago, I have a particular interest in the subject of personal privacy. During my 5 years of service on the Foreign Operations and Government Information Subcommittee, I participated in several investigative hearings into this important area. Today, as ranking minority member of the Government Operations Committee, I am very happy to lend my strong support to a bill which insures that

Federal Government agencies protect individuals' rights to privacy when dealing with information about people.

The bill does this in two ways:

First, it mandates that agencies disclose an individual's records to other persons or other agencies only with the written consent of that individual, unless the disclosure would be for a purpose which had been endorsed by the Congress or published in the Federal Register. Whenever the Government asks someone for information about himself, according to the bill, it would have to inform him of the disclosures which had been published as permissible.

Second, the bill provides that individuals shall have access to all Government records maintained about them, and shall have the right to petition agencies to correct any misstatements in those records. Agencies would have to make the changes requested or note on the records that the changes had been sought, but that the Government disagreed with them.

All Federal records pertaining to individuals would be covered by these provisions, except for national security information, investigatory material compiled for law enforcement purposes, other criminal justice records, Secret Service and CIA files, and statistical data.

To make sure that Government agencies fulfill their responsibilities under this legislation, the bill permits individuals who are injured by Government agency's failure to comply with the law to bring suit against the agency in Federal court. A successful complainant could be awarded actual damages and attorney's fees by the judge.

Mr. Chairman, this is landmark legislation in an area of concern to all Americans. I urge its enactment.

Mr. ERLENBORN. Mr. Chairman, I yield 3 minutes to the gentleman from Maryland (Mr. Gude).

(Mr. Gude asked and was given permission to revise and extend his remarks.)

Mr. GUDE. Mr. Chairman, as a cosponsor of this legislation, I am indeed gratified that it is finally receiving the floor consideration which it should.

I want to commend the chairman of our subcommittee, the gentleman from Pennsylvania (Mr. Moorhead); the ranking member, the gentleman from Illinois (Mr. Erlenborn); and, in particular, the gentleman from California (Mr. Goldwater), the gentlewoman from New York (Ms. Abzug), and the gentleman from New York (Mr. Koch) who are also cosponsors of this legislation. They have been a driving force toward its consideration and in bringing it to the point where we find it at this moment.

The chairman of the subcommittee has very well outlined exactly what this legislation does. It is long overdue. This is the kind of attention that Government records have needed for some period of time. I think matters which we consider routine and perfunctory are very often hidden under agency directives, rules, and regulations, and we assume what is normal to us on the Hill to be what is normal throughout the Federal Government.

Increasingly, as the society and the Government have grown more complex, the maze of Federal activity and regulation have intensified, and the individual citizen has had to make increasing concessions to

the imperatives of the Federal bureaucracy. The quantity of Federal paperwork alone, for example, has reached such proportions, that the House felt the need last month to authorize the establishment of a Commission on Paperwork to study the problem and find ways of reducing the burden which bureaucracy imposes on the citizen.

The level of regulatory activity which touches on the lives of individual citizens has also increased. Seat belt standards, now repealed, safety and health standards, labeling and advertising standards, while important Government tools to correct serious problems we have, all intrude on the freedom of the individual in some small way.

Certainly the demands of a complex technological society call for some concessions, but we have before us today an opportunity to help balance the recent trend of legislative activity by enacting legislation to help restore individual rights and individual privacy. This bill imposes limits on what the Government can do with individual data, and it imposes obligations on the Government to the subjects of the data, and in doing so it helps to maintain the balance of individual freedom and privacy which we all cherish.

Symbolic of this balance is the controversy over the use of social security numbers for identification purposes. While such a proposal may make sound technological sense, to many citizens it implies removal of an important element of their privacy and individuality. This question is not dealt with in this bill, but some of the same principles are—the right of the individual to maintain his privacy and personal identity.

Beyond these questions of principle, the bill also has substantive significance for many citizens who feel, rightly or wrongly, that they have not received a "fair deal" from their Government.

Mr. Chairman, I would like to quote the experience which one veteran had in regard to the Veterans' Administration. He was unable to obtain compensation and relief for injuries he had received while serving his country abroad, and yet he was unable to look at his records in the Veterans' Administration files. He finally had to obtain legal counsel in order to get access to his files, and he found the reason the Veterans' Administration had denied his obvious need was because certain records that were in his file actually belonged to another veteran who had a similar name.

This may seem to be a very small thing, but this is the type of action which can occur in situations when we in Congress have not enacted regulations to provide for the overseeing of Federal records, which can sometimes be buried under a lot of bureaucratic redtape which denies the citizen the access to which he is entitled.

Mr. Chairman, I am going to offer two amendments to this bill at the appropriate time. They are amendments which I was unable to offer in the committee, because of the pressure of business when we were reporting the legislation to the floor. The first has to do with medical records.

This first amendment would clarify one item that I believe to be ambiguous in intent, in restricting the circumstances under which individuals would be granted disclosure by Federal agencies. It was the intention of the committee to exclude information which would be vital to the health or safety of an individual.

I believe that the current language in the bill is vague in this regard, in that it would permit such disclosures without prior permission, unless it is an emergency case. It does not make clear to whom the information would be disclosed.

The second amendment I would offer is one that would establish a Privacy Commission, which I believe is a vital necessity if the privacy legislation we are enacting is to become a meaningful statute. Clearly, the enactment and maintenance of successful privacy standards would hinge on the degree of cooperation provided by Federal agencies which have to implement the program.

The Privacy Commission which I will propose will coordinate and assist in these efforts, and it would be an important goal for gaining the necessary agency cooperation in order to make this legislation meaningful in the service of American citizens.

Mr. Chairman, I will offer these two amendments at the appropriate time.

Mr. HOLIFIELD. Mr. Chairman, will the gentleman yield?

Mr. GUDE. I will be glad to yield to the chairman of the full committee.

Mr. HOLIFIELD. Does the gentleman's amendment of the privacy bill follow the words of the Senate provision?

Mr. GUDE. I have not compared them word for word, Mr. Chairman, but I believe it does.

I urge the passage of this legislation.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I yield 5 minutes to the gentleman from Arkansas (Mr. Alexander), a member of the subcommittee.

(Mr. Alexander asked and was given permission to revise and extend his remarks.)

Mr. ALEXANDER. Mr. Chairman, on June 19, following hearings on the Federal Government's use of telephone monitoring and lie detection devices conducted by the Subcommittee on Government Information, I stated that it appears our Government has been overcome by a snooping mania and that we must find the medicine to cure this disease. H.R. 16373, the Privacy Act of 1974, is a good dose of such medicine.

I was alarmed to discover in those hearings that it is literally possible to have every home in America bugged.

Mr. Chairman, I am convinced that Americans do not want to be a part of one big party line. If present Government preoccupation with spying on its citizens continues, George Orwell's fictional fishbowl existence and "Big Brother" era in his book "1984" may very well occur.

H.R. 16373 provides basic safeguards for the individual to help remedy the misuse of personal information by the Federal Government, and reasserts the fundamental rights of personal privacy that are derived from the Constitution. At the same time, it recognizes the legitimate need of the Government to collect, store, use, and share among various agencies certain types of personal data, but under a framework of law to protect the citizen.

Like the Freedom of Information Act Amendments, H.R. 16373 also recognizes that certain areas of Federal records are of such a

highly sensitive nature that they must be exempted from some of its provisions.

The Privacy Act provides for the exercise of civil remedies by individuals against the Federal Government through the courts to enforce their rights. Provision is made for the actual collection of damages by the individual against the Government if the infraction was willful, arbitrary, or capricious. Penalties are also provided for the unauthorized knowing and willful disclosure of identifiable material by a Government officer or employee by a fine of not more than $5,000. Criminal penalties and fines would also be imposed on persons requesting or obtaining any such individually identifiable record under false pretenses.

The bill attempts to strike that delicate balance between two conflicting and fundamental needs—on the one hand, the need for a maximum degree of privacy and control over personal information the individual American furnishes his Government, and, on the other hand, the need for information about the individual which the Government finds necessary to carry out its legitimate functions.

Over 40 years ago, Supreme Court Justice Louis Brandeis, in his famous dissent in the case of Olmsted against United States, said:

> Every unjustifiable intrusion by the government upon the privacy of the individual whatever the means employed, must be deemed a violation of the fourth amendment.

He further stated in terms relevant to current wholesale abuses of power that:

> Experience should teach us to be most on guard to protect liberty when the government's purposes are beneficient. Men born to freedom are naturally alert to repel invasions to their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding . . .

Let us talk a moment on the concept of privacy. Privacy is the ability to be confident of security in our homes, persons, and papers. It is not only the bedrock of freedom. Privacy is the very essence of democracy. If we cannot speak or transact business without being snooped on by hordes of bureaucrats—we soon will not be able to speak or transact business without government permission.

In my opinion, events in recent years have brought about a chilling effect on the exercise of first amendment rights. It is now time for a defrosting. Every American must insist that government is the servant of the people—not our master.

In his first speech as Chief Executive, President Ford pledged his personal and official dedication to the individual right of privacy, in declaring that "there will be hot pursuit of tough laws to prevent illegal invasion of privacy in both government and private activities."

H.R. 16373 is a first step in that pursuit. I strongly urge my colleagues to support this legislation.

Mr. Erlenborn. Mr. Chairman, I yield such time as he may consume to the gentleman from Indiana (Mr. Hudnut).

Mr. Hudnut. I thank the gentleman for yielding.

(Mr. Hudnut asked and was given permission to revise and extend his remarks.)

Mr. Hudnut. Mr. Chairman, I rise in support of H.R. 16373, the Privacy Act of 1974. While there will be amendments offered to

strengthen this bill, I feel the Committee on Government Operations has done a good job in bringing this legislation before us. There is a great need for statutory guidelines to protect the privacy of individuals by regulating the Federal Government's collection, maintenance, use, or dissemination of personal, identifiable information.

In this computer age, it is easy to obtain information about an individual and along with many others I am concerned over the extent to which citizens' privacy is being invaded. We see this in the accumulation of personal data in computer banks and other such means which constitute a threat to the privacy of every American citizen. There are some who look upon individual tax returns as the greatest source of such information.

Earlier this year I cosponsored a bill (H.R. 10977) to provide further restrictions on accessibility to individual tax returns. The assurance provided the American people that information voluntarily given on tax returns will be carefully protected from disclosure and improper use is one of the basic concepts underlying this country's system of collecting taxes and I want to assure that protection. I am hopeful that the Ways and Means Committee will take specific action on that measure.

In the meantime, H.R. 16373 provides a series of basic safeguards for the individual to help remedy the misuse of personal information by the Federal Government and reassert the fundamental rights of personal privacy of all Americans that are derived from the Constitution of the United States. At the same time, it attempts to strike that delicate balance between the right of individuals for a maximum degree of privacy over the personal information he furnishes his Government and the need of the Government for information to carry out legislative functions.

Mr. ERLENBORN. Mr. Chairman, I yield 5 minutes to the gentleman from California (Mr. Goldwater).

(Mr. Goldwater asked and was given permission to revise and extend his remarks.)

Mr. GOLDWATER. Mr. Chairman, I thank the distinguished minority member on the subcommittee, the gentleman from Illinois (Mr. Erlenborn) for allowing me the privilege of speaking in favor of this particular legislation before us today, which has been long in coming and long overdue.

This particular piece of legislation is the result of a strong bipartisan effort in the House of Representatives. The efforts of my colleague, the gentleman from New York (Mr. Koch) in behalf of an individual's right to privacy, are well known and were extremely important in the preparation of this legislation. Equally significant were the efforts of the members and the staff of the Subcommittee on Foreign Operation and Government Information of the Committee on Government Operations and, particularly, the subcommittee chairman, the gentleman from Pennsylvania (Mr. Moorhead) who was most diligent in pursuing this very difficult task, and who was assisted quite ably by the ranking Republican member, the gentleman from Illinois (Mr. Erlenborn). They are both to be commended for this excellent piece of legislation.

This legislation, as I said, has been long in coming, and is only here today because of the persistent efforts of not only members of the

Committee on Government Operations, but also many Members of the House of Representatives, as well as Members of the other body, not to mention the private sector, educators, members of private organizations, and just plain people, and it certainly would be most fitting to mention the fine efforts by our President of the United States, Gerald R. Ford, and his Committee on the Right of Privacy.

Mr. Chairman, my concern for privacy is a long-standing one. The right to privacy is a derivative right. It is not specifically mentioned in the Constitution, as are the general rights of life, liberty, and the pursuit of happiness, nor is this subject mentioned in the Bill of Rights. But none of these would have had the content that we know them to have without the element of privacy being present. It is an essential, inherent element of our inalienable rights.

The concern for protecting personal privacy as it relates to personal information is fairly recent in its origin. The rapid growth of our population and the rise of massive urban centers, the advent of modern communication and electronic technology, and the rise of the computer, have brought a basic change in our society. Massive amounts of personal information can be conveniently and economically collected, stored, and used. The individual is no longer directly involved in the modern personal information transaction process. Many information practices have been developed and adopted because they were convenient, technologically feasible, and cost-effective. The individual actually became an impediment in these new processes. As he began to protest his exclusion and try to protect himself from the injury and damage that occasionally resulted, he found he had no legal rights to fall back on.

Mr. Chairman, the Federal Government has a relentless appetite for information. There seems to be a direct correlation between the continued growth of Government and the continued growth of privacy invasion.

The Federal Government, as we enact more and more programs, has a need to collect more and more information in order to administer these programs. So it is with this piece of legislation that we are trying to strike a balance between the need to know in order to successfully and correctly administer Government programs, and the rights of an individual to be left alone, to control his own personal life. This particular bill undertakes to redress this disastrous imbalance.

The Federal Government is required to permit an individual to know what records it has pertaining to him. It introduces the element of active consent as a requirement before information that is collected for one purpose can be put to a new use. It permits an individual to have copies of files about him and to correct or amend erroneous portions of them.

Finally, it requires the Government to keep records accurately and securely in accordance with specific, published regulations.

The CHAIRMAN. The time of the gentleman has expired.

Mr. ERLENBORN. Mr. Chairman, I yield 2 additional minutes to the gentleman from California.

Mr. GOLDWATER. It is noteworthy, Mr. Chairman, that this Privacy Act of 1974 prohibits the Federal Government from maintaining secret personal information systems. This bill is an important major

first step in the restoration of the individual's right to privacy, and I would caution and suggest to my colleagues that as we pursue further legislation in other areas, we constantly be vigilant that we do not undermine this effort today, that we take into consideration in new legislation, enabling legislation, the rights of the individual to his privacy. It is time that we insert human rights into the programs and the programers. It is time that we insert privacy rights into the policy of our agencies. It is time that we instill a spirit of concern for our liberties. We must reestablish and I think we do so with this legislation—the right to be left alone for the people of this country.

Mr. Chairman, I urge my colleagues to support this legislation.

Mr. SYMMS. Mr. Chairman, will the gentleman yield?

Mr. GOLDWATER. I yield to the gentleman from Idaho.

Mr. SYMMS. I thank the gentleman for yielding.

(Mr. Symms asked and was given permission to revise and extend his remarks.)

Mr. SYMMS. Mr. Chairman, I wish to associate myself with the remarks of the gentleman from California (Mr. Goldwater).

I should like to commend the gentleman from California for his efforts that he has made on behalf of this Privacy Act which we have here before the House today. I would say to the gentleman in the well I thank him for his support, effort, and leadership on it and hope that it is successful today, as this Privacy Act offers some protection for people from big brother government snoopervision.

Mr. GOLDWATER. I thank the gentleman and commend him also for his support and active participation on the Republican Task Force on Privacy, which issued what I considered a very comprehensive report and bibliography this past year.

The CHAIRMAN. The time of the gentleman has expired.

Mr. ERLENBORN. Mr. Chairman, I yield such time as he may require to the gentleman from California (Mr. Rousselot).

(Mr. Rousselot asked and was given permission to revise and extend his remarks.)

Mr. ROUSSELOT. Mr. Chairman, I want to commend my colleague, the gentleman from California (Mr. Goldwater) for the effort he has put forward on this issue, and our subcommittee chairman for his work on this issue.

Mr. Chairman, as one of the original cosponsors in this Congress of right to privacy legislation, I rise in support of H.R. 16373, the Privacy Act of 1974.

This is a comprehensive bill which is intended to protect the privacy rights of individuals by regulating the Federal Government's collection, maintenance, use or dissemination of personal, identifiable information.

Through my committee assignments on Banking and Currency, and Post Office and Civil Service, I have become particularly aware of the need for the protection of an individual's privacy rights with regards to bank records and census data. Very strict care must be taken to protect the confidentiality of these records and insure that the information is used only for proper purposes. Since the census questions have become more detailed and extensive, the dissemination by the Census Bureau of statistical data must be more closely regulated in order to

protect the individual from being identified by that data. H.R. 16373 does provide proper safeguards in this area.

Mr. Chairman, I have sponsored legislation, H.R. 10021, the Right to Financial Privacy Act. My bill would protect the constitutional rights of citizens by prescribing procedures and standards governing the disclosure of financial information by financial institutions to Federal officials or agencies. The bill we are discussing here on the floor today does not regulate the collection of information by the Federal Government other than to prohibit any agency from maintaining any record concerning the political or religious belief or activity of any individual unless expressly authorized by statute or the individual himself. I realize that by the very nature of the subcommittee's—the Foreign Operations and Government Information Subcommittee of the House Government Operations Committee—jurisdiction it could not get into this area of regulating the activities of the Federal Government specifically with regards to obtaining individual bank records, so I hope that our concern about privacy rights will not stop with the passage of this one bill, H.R. 16373.

I urge support of H.R. 16373 with the hope that in the next Congress, we will give further attention to areas that need to be specifically considered in order to afford our citizens full protection from the violation of their privacy rights by the Federal Government. Of these areas, one of the most important is, I believe, the legislation which I have sponsored to preserve the confidential relationship between financial institutions and their customers and the constitutional rights of these customers.

Mr. ERLENBORN. Mr. Chairman, I yield such time as he may require to the gentleman from Minnesota (Mr. Frenzel).

(Mr. Frenzel asked and was given permission to revise and extend his remarks.)

Mr. FRENZEL. Mr. Chairman, I rise today in enthusiastic support of H.R. 16373, The Privacy Act of 1974. In this bill we are regulating the collection, maintenance, and use of by Federal agencies of information concerning American citizens.

I hope this bill will be the first of a wave of privacy oriented legislation which the Congress will consider in the next few years. Therefore, we must be very careful in laying a foundation for future reforms. Other areas which clearly need attention are the protection of constitutional freedoms for Federal employees, limitations upon distribution of federally collected information, and strict regulations upon the types and use of surveillance tactics employed by Federal agencies. Beyond our limited Federal perspective, we must also seriously examine the activities of private information and collection services.

Since I entered this body in the 92d Congress I have proposed over a dozen bills relating to questions of individual and financial privacy and domestic intelligence. Along with most Members, I am committed to guaranteeing the rights implicit in the 1st, 4th, and 14th amendments. This bill, H.R. 16373, is a good start.

I urge that we pass this bill, with the inclusion of a Federal Privacy Commission and some changes in the civil procedure and criminal penalties sections. It is only a start, but it will be a good base for future laws to protect the personal privacy of all Americans.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, at this time I yield 5 minutes to the gentleman from Missouri (Mr. Ichord).

(Mr. Ichord asked and was given permission to revise and extend his remarks.)

Mr. ICHORD. Mr. Chairman, as its title—the Privacy Act of 1974—and the prefatory findings indicate, it is the commendable purpose of the measure to protect the individual against the misuse of official information. To that end the act would add a new section to what is now commonly known as the Freedom of Information Act (5 U.S.C. 552). The new section, to be designated section 552a, would impose conditions upon the disclosure of official information, and would give individuals affected access to such information so as to permit them record.

The committee which reported the measure and the gentleman from Pennsylvania (Mr. MOORHEAD) who chaired the subcommittee which had the measure under consideration, are to be commended for the professional manner in which they have sought to deal with this extremely complex and difficult subject.

The "right" of privacy has been said to be the right of the individual "to be left alone." It is without doubt a right inherent in our libertarian system. While it is said that this right is not explicitly asserted in our Constitution, it does however find expression in certain related provisions and in the basic philosophy which prompted the adoption of the Constitution itself. By that instrument those freedoms and liberties were reserved to the individual which were not deemed essential to the coexistence of man in society. Hence, like other rights, the right of privacy is not deemed an absolute right.

Logically, the absolute right of privacy could be fully asserted only in a state of anarchy.But even in such a state, if extended to its outer and extreme limits, the exercise of any such absolute right must necessarily collide with the rights of other individuals. The resulting conflict would consequently result in the destruction of the rights asserted by each. It necessarily follows that if the right of privacy is to be recognized as a legitimate claim in an ordered society, it must be subject to limitations and must be conditioned upon the rights of others and exercised consistently also with the rights of the public.

What we are dealing with in statutes of this type is thus necessarily a balancing process by which we seek to resolve the right of the individual to be left alone with the public and other individual rights "to know." For it is a fact that such latter rights are equally recognized by the Constitution, although in a sense they may collide, with the individual's "right of privacy." The first amendment rights of freedom of speech and of the press, for example, intrude upon an individual's right of privacy, but they are rights which are essential to the administration of Government and to the free functioning of our libertarian and democratic institutions. Moreover, the individual's right to privacy must be conditioned by that which is consistent with the continued existence and protection of that Nation and its constitutional system upon which the vitality of the right itself must ultimately depend.

It appears to me that the bill before us has generally resolved the conflict between the rights of the individual and the public and other private rights with considerable success. I propose today to offer only

two amendments to the bill which are directed toward clarifying certain aspects of the measure's impact upon our intelligence services, particularly in relation to the acquisition and use of information which is essential to the maintenance of the national and internal security. On their adoption I shall support this measure.

First, however, I should like to express my concern over an ambiguity inherent in the provisions of the proposed subsection (b), at page 22, line 10, relating to conditions of disclosure. This subsection would, subject to the exceptions therein set forth, generally prohibit an agency from disclosing to any person information about an individual without the individual's prior written consent. The subsection would generally authorize only interagency and intraagency disclosures for authorized law enforcement activities, but does not appear to contain any explicit provisions authorizing certain essential disclosures outside official agencies which would be clearly required if certain vital security programs maintained by the Government are to be effectively carried out. These include, for example, the effective maintenance of the industrial security, industrial defense, atomic energy, and port and vessel security programs. Defense contractors and others involved in the receipt of classified information and related information about individuals are mainly private employers.

I am informed, however, that the provision of subsection (b) (2) which would except from the prohibition the communication of information therein described as "for a routine use," is intended by the sponsors of the legislation to permit such essential disclosures beyond the bounds of the particular agencies involved. If this is effectively accomplished by the language of this exception, it may well be that a specific clarifying amendment is unnecessary on this aspect of the bill. It is my hope that any such ambiguity as may exist on the reach and meaning of this provision, can be obviated in colloquy with the sponsors of the measure at the appropriate time.

On the other hand, I deem it necessary to offer a specific clarifying amendment to the provisions of subsection (e), paragraph 4. This section commences at page 26, line 18, of the bill. The particular paragraph of this subsection to which the amendment will be offered is at page 28, line 13. This subsection and paragraph prohibits an agency from maintaining any record, and I quote, "concerning the political or religious belief or activity of any individual, unless expressly authorized by statute or by the individual about whom the record is maintained." We may well recognize that the purpose of this provision is commendable and legitimate in prohibiting the disclosure of records with respect to conventional political and religious beliefs and activities. However, in its present form it is clear that the provisions can be construed to cover activities which are properly within the scope of legitimate law enforcement. I am assured that the authors of this measure have not intended the provisions to foreclose this proper purpose.

The terms of the broad prohibitions on maintenance of records relating to "political" and "religious" activities would, for example, embrace the activities of the Communist Party and similar groups, which, although generally recognized as conspiratorial or clandestine, are nevertheless commonly described as "political." Similarly, cer-

tain sects within the Black Muslim movement, which have been described by the Director of the FBI as endangering the internal security, may claim protection under this clause as a "religious" activity.

Although those records of political or religious activity which are "expressly authorized by statute," are excepted from the prohibitions of this paragraph, this is not adequate to exempt the activities of such subversive groups as I have indicated. I know of no existing or enforceable statute which expressly and generally authorizes any particular agency to maintain the records of political or religious activities of subversive groups. I would therefore amend this paragraph by striking out the period after the word "maintained" and add the following:

"; provided, however, that the provisions of this paragraph shall not be deemed to prohibit the maintenance of any record of activity which is pertinent to and within the scope of a duly authorized law enforcement activity."

I believe this clarifying amendment would obviate any ambiguities as to the reach of the prohibition, and would serve to eliminate any adverse litigation on the subject.

The second and final amendment, which I propose to offer to the measure, would affect the provisions of paragraph (2) of subsection (k), at page 34, line 7. This section deals with certain specific exemptions that may be made to the disclosure requirements of the act, particularly with respect to those investigatory files or material which the Act would otherwise require the agencies to disclose to an individual by the provisions of subsection (d). While the provisions of paragraph (2) of subsection (k) would permit the agency to exempt from the mandatory disclosure requirements of subsection (d) investigatory material compiled for law enforcement purposes to the extent it is not now open to public inspection under the provisions of existing law, that is, section 552(b)(7) of title 5, United States Code, it would appear to me that under this paragraph there is a question whether the agency could exempt from public disclosure the identity of individuals and information pertaining to those, for example, who are members of such organizations as the Communist Party and other revolutionary groups having similar objectives.

In view of the fact that there are literally tens of thousands of individuals who are involved in such revolutionary organizations, to require such agencies of the Government as the FBI and the defense intelligence agencies to disclose investigatory material pertaining to such individuals on request, would not only have the effect of literally immobilizing the agencies in the effective execution of their essential and vital work, but would greatly impair, if not destroy, their functioning. The research which would be involved, the extensive correspondence required, and the litigation which would likely ensue as a result of the thousands of requests that would conceivably and very likely pour into the agencies would wreak havoc upon the agencies. Moreover, to permit the indiscriminate raiding of investigatory files, the maintenance of which in confidence is so essential to the protection of the national and internal security, would also destroy their usefulness by revealing the extent of coverage and the method and adequacy of operation of our intelligence forces. Any such result is wholly unnecessary to the attainment of the objectives and purposes of the bill.

63-619—76——58

I would thus amend paragraph (2) of subsection (f) by striking the paragraph in its present form and amend it to read as follows:

On page 34, strike lines 7 through 11 and insert the following in lieu thereof:

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section; provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

Thus by its terms the amendment would fully protect the individual by requiring the disclosure to him of relevant investigatory material in the system of records—other than that within the scope of subsection (j)(2)—when, as a result of the maintenance of such material, he is denied any right, privilege, or benefit to which he would otherwise be entitled by Federal law, or for which he would otherwise be eligible. In such event disclosure is limited to the extent necessary to protect the identity of a source who furnished information to the Government under a promise that the identity of the source would be held in confidence.

This amendment very properly serves the purpose of protecting the investigatory material from being raided by the thousands and perhaps tens of thousands of persons who may seek to do so for no legitimate or excusable purpose.

Hence the right of privacy of the individual is protected, without diminution, to the extent of his legitimate requirements. It shall be recognized that the amendment does not affect the requirements of subsection (b) of the bill, which prohibits disclosure of information beyond the legitimate uses of the Federal agencies maintaining them. Thus the privacy of the individual remains protected by the amendment consistently with the attainment of the purposes of the bill and the national security interest.

There is one final point to which I should direct attention, regarding both the wording of this and my prior amendment, in the use of the term "law enforcement" as applied in the context of these amendments and the bill as a whole. In referring to a "law enforcement activity" and "law enforcement purposes," I am, of course, using the expression "law enforcement" in its general meaning and in the broadest reach of the term. I include within that term those purposes and activities which are authorized by the Constitution, or by statute, or by the rules and regulations and the executive orders issued pursuant thereto. Thus, the investigatory material maintained shall include, but not be limited to, that which is compiled or acquired by any Federal agency in connection with and for the purpose of determining initial or continuing eligibility or qualification for Federal employment, military service, Federal contracts, or access to classified information.

I want to emphasize—so that there is no misunderstanding—these changes are designed to protect only legitimate national or internal security intelligence and investigations, and no records or files shall be kept on persons which are not within constitutional limitations. Let

the legislative history be explicit. None of these changes are intended to abridge the exercise of first amendment rights. The rights of Americans to dissent in a lawful manner and for lawful purposes must be preserved.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, we did discuss these two questions, I will say to the gentleman from Missouri, and we did say it was our understanding that under the gentleman's amendments no file would be kept of persons who are merely exercising their constitutional rights, as the gentleman stated.

Mr. ICHORD. The gentleman is exactly correct.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I yield 5 minutes to the gentleman from New York (Mr. Koch), who has been so very active in the privacy of information field.

(Mr. Koch asked and was given permission to revise and extend his remarks.)

Mr. KOCH. Mr. Chairman, first I want to thank the distinguished gentleman from Pennsylvania, my good friend (Mr. Moorhead), who is responsible for so much of the language incorporated into this bill and for the efforts necessary to bring it to the floor.

I just want to take special note of what he has done on behalf of privacy as well as take note of the enormous efforts on the Democratic side by the gentlewoman from New York (Ms. Abzug) and on the Republican side by the gentleman from Illinois (Mr. Erlenborn) and the gentleman from New York (Mr. Horton).

Rather than restate the provisions of the bill which have been so amply set forth by a number of the speakers, I would rather simply comment on the fact that this kind of legislation which relates to the privacy of the individual, protecting that individual from Government, has the support of those who are conservatives and those who are liberals.

They have indicated that support by rising in the well this very afternoon, on both sides of the political spectrum and both sides of the aisle.

That is not to say that this bill is a perfect bill. I do not know of any perfect legislation. It may be there have been occasions when there has been legislation never requiring an amendment of any kind brought to this floor and passed, but I am not aware of it.

This bill, however, is a very good bill. There are amendments that will be offered, some that I support, some that I oppose; but the thrust of most of those amendments and the nature of those amendments is intended by those offering them to improve the bill. We may disagree on whether they do or do not; but the persons involved in most of the amendments want to protect privacy and that is the key and very important to understand when we discuss those particular amendments.

There is an area that ought to be covered which is not by this bill. If I had my way, I certainly would have it in the bill; that area relates to law enforcement agencies which are, frankly, not covered adequately under this bill. The reason for that is that the Committee on the Judiciary has before it legislation which relates to the criminal data banks of law enforcement agencies. I know that that great committee with its distinguished chairman (Mr. RODINO) and the subcommittee chairman in charge of that subject, the gentleman from California (Mr. Edwards) are very concerned about the rights of

privacy. So I have no doubt that the legislation which I am informed they intend to bring to the floor, hopefully early in the next session, will cover that data not covered under this legislation, pertaining to law enforcement agencies.

What this legislation does do is open the Federal files in so many areas. Millions of files that are now not available to the public would become available to the public. I am not saying available to the public in terms of seeing somebody else's file, but seeing one's own file, seeing whether the material in there is relevant, seeing whether it is accurate, seeing whether it is current, and if it is not, providing the mechanism whereby that can be corrected.

This is landmark legislation. This is legislation in which I take great pride having espoused it in February of 1969, and later with my good friend, the gentleman from California, Mr. Barry Goldwater. In my own district we refer to the legislation as the Koch-Goldwater bill, and in his district as the Goldwater-Koch bill; but the fact is that while the initial legislation was ours, it has been subjected to extensive review and amendment by the committee and improved upon in a number of ways. This legislation is now the joint work product of many people. I am proud to be one of those who brought this legislation to this point, where its passage seems assured.

Again, I want to express my deep appreciation to the chairman, Mr. Moorhead, the members of the committee, its brilliant staff without whose hard work, we would not be here tonight, and to my partner on this legislation, Barry Goldwater, Jr.

Mr. BIAGGI. Mr. Chairman, I rise in strong support of this legislation. I feel that passage of this bill today will represent a significant victory in the battle against unlawful and dangerous intervention by the Federal Government in the private lives of the average American citizen.

While the fourth amendment to our Constitution clearly spells out the right of the individuals to privacy in recent years, the Federal Government has intensified their efforts to superimpose themselves into the lives of the individual. Many people pointed to these dangerous actions by the Government as the fulfillment of the Orwellian theory of "Big Brother" as contained in his masterpiece, "1984."

What we are considering today is comprehensive legislation which will take a number of steps to protect the individual from the power of the Federal Government. Perhaps the strongest area of controversy concerns the maintaining of nonessential records by Government agencies against individuals. This legislation addresses itself decisively to this problem in the following ways:

It permits an individual to be aware of and have access to all personal information records compiled by Government agencies, except in cases where these records are needed for law enforcement and national security.

It allows the individual to control the transfer of personal information records from one Government agency to another.

It further specifies the extent of records which can be maintained by the Federal Government, and specifically prohibits keeping of records which contain a person's political and religious beliefs unless clearly provided for by law.

Finally, this legislation sets a new and important precedent by allowing for a civil remedy to be acquired by individuals in instances

when they have been denied access to their records or whose records have been kept or used in violation of the provisions of this law. The individual will have the right to bring suit as well as the ability to collect damages if it can be established that such actions were taken capriciously by the Government.

I feel a sense of personal relief in the realization that the Congress has seized the initiative in this area. Many of us sitting here today have been the target of unlawful Government intervention in our personal activities. I feel that the recent abuses of power disclosed in the Watergate hearings may have provided a special impetus for the development of this legislation. One only has to read these hearings to discover the extent to which certain Government agencies either were manipulated or on their own took steps to discredit those individuals they view with suspicion or fear.

On the same token I am pleased to see that certain conditions were contained in this bill. As a former law enforcement officer, I know the value of maintaining information about potential or actually dangerous groups. There are dangerous and anarchistic elements in this society which merit the close attention of law enforcement personnel and I applaud the fact that we are not tying the hands of law enforcement as they work to uphold the law of the land.

Mr. Chairman, the legislation we are considering today is both necessary and vital to the American people. We are a free nation and the strength of our Nation derives from the rights of the individual to freedom and privacy. Many Americans have become justifiably alarmed in recent years by the increased activities of the Federal Government in the area of maintaining personal records and information. We are today striking a blow against the potential of tyranny in this Nation and I am pleased to rise in support of this bill which can only enhance and strengthen the bonds of freedom which exist in this Nation.

Mr. Regula. Mr. Chairman, I rise in support of H.R. 16373, the Privacy Act of 1974.

In April of this year I joined with my colleagues Messrs. Goldwater and Koch in participating in a special order to discuss the need for the establishment of a national privacy policy. A singular point or theme emerged from that discussion; one of the basic tenants of our system of law is the right to confront a witness or an accuser and to cross-examine him in order to elicit the truth.

In recent years computers, photocopiers, and other technological advances have made the storage and retrieval of information about citizens fast and relatively inexpensive. Almost without notice and in the name of efficiency our technological progress has moved us toward the "big brother" supervision predicted in George Orwell's book "1984."

Today, an individual does not really know who has information about him, or how many agencies or corporations are using it or for what purposes. There is no mechanism for providing explanations or to add mitigating facts. And, even more important there are no limits on what can be collected either by Government or the private sector.

Information is collected on academic achievement, credit ratings, health, judicial records, employment history, birth and marriage records, military records, tax returns and census records, to name a few.

The written word, film, or computer punch card bears witness as eloquently as the spoken word. The right of access to and challenge of records by the subject of the information obtained in those records could, if exercised under the same or similar rules, only instill confidence in aid our governmental process.

This bill, H.R. 16373, would provide the Government with the tools it needs to regulate, collect, maintain, use, and disseminate personal, identifiable information. It would provide individuals with the safeguards they need to prevent misuse of this information.

Like the Freedom of Information Act, which I am sure this Congress will pass in one form or another, this bill is a significant step toward open government.

I urge my colleagues support for passage of this bill.

Mr. BROYHILL of North Carolina. Mr. Chairman, I strongly support the passage of H.R. 16373, the Right to Privacy Act. Earlier this year, I cosponsored H.R. 15524, a forerunner of this legislation.

I feel, as do many Members of Congress, that there is a growing capacity for major violations of the privacy of Americans, as the Federal Government increases its collection and use of data furnished by citizens for specific governmental purposes. Safeguards are needed to insure that the personal information obtained by the Government, for legitimate purposes, is not misused. Recently, we have witnessed flagrant violations of the constitutional rights of some of our citizens by the Federal Government. We should enact legislation now to insure that these individual rights are never again violated.

While there can be no absolute protection of privacy in any society, I believe H.R. 16373 provides the necessary safeguards for greater protection of private records. Perhaps the greatest protection afforded the individual is his right to have access to his records, and to control the transfer of any personal data from one Federal agency to another for nonroutine purposes. Additionally, the bill will require the disclosure by every Federal agency of certain identifying characteristics about virtually all systems of records under their control, to insure that no "secret" Government system of records is created.

H.R. 16373 would also permit individuals access to civil court action against the Federal Government should their rights be violated. Provision is made for the awarding of actual damages to an individual, if the Government is shown to have acted willfully, arbitrarily, or capriciously in violating the provisions of this act. Criminal and civil penalties could be levied against individuals who disseminate or seek to obtain personal information contained in Federal files.

Mr. Chairman, it is essential that the Federal Government, the largest repository of personal records in the country, do everything possible to safeguard these files and to protect the rights of every American citizen. H.R. 16373 contains these safeguards and protections. I will support this measure and I urge my colleagues to do likewise.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I have no further requests for time.

The CHAIRMAN. Pursuant to the rule, the Clerk will now read the committee amendment in the nature of a substitute printed in the reported bill as an original bill for the purpose of amendment.[1]

[1] See p. 258.

Mr. MOORHEAD of Pennsylvania (during the reading). Mr. Chairman, I ask unanimous consent that the bill be considered as read, printed in the Record, and open to amendment at any point.

The CHAIRMAN. Is there objection to the request of the gentleman from Pennsylvania?

There was no objection.

AMENDMENTS OFFERED BY MR. MOORHEAD OF PENNSYLVANIA

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I offer two amendments, and I ask unanimous consent that my amendments be considered en bloc.

The CHAIRMAN. Is there objection to the request of the gentleman from Pennsylvania?

There was no objection.

The Clerk read as follows:

Amendments offered by Mr. Moorhead of Pennsylvania: Page 22, lines 19 and 20, strike out "in any rule promulgated".

Page 27, line 8, immediately after "(2)" insert "subject to the provisions of paragraph (5) of this subsection,".

Page 28, line 12, strike out "and"; on line 16, strike out the period and insert in lieu thereof "; and"; and immediately after line 16, insert the following new paragraph:

(5) at least 30 days prior to publication of information under paragraph (2)(D) of this subsection publish in the Federal Register notice of the use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

Mr. MOORHEAD of Pennsylvania (during the reading). Mr. Chairman, I ask unanimous consent that further reading of the amendments be dispensed with. They have been distributed to the minority side, and I do not think further reading of the amendments is necessary.

The CHAIRMAN. Is there objection to the request of the gentleman from Pennsylvania?

There was no objection.

(Mr. MOORHEAD of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, this amendment has also been discussed in advance with the minority side. Its purpose is to tighten up the part of the bill under which a Federal agency makes its determination as to the "routine purpose" for which records contained in a system of records are to be used or intended to be used. As I explained in earlier remarks, "routine" uses of personally identifiable information permit an agency to transfer such records without obtaining the individual's consent—within the agency or between agencies—in the "routine" conduct of Government business.

It is essential, however, that this "routine" authority is not abused so as to circumvent the basic purposes of this law. Under the present language of the bill, an agency—under subsection (e)—may publish in the Federal Register a list of each "routine purpose" for which records in an information system are used. The danger is that there is no check on the agency—except congressional oversight—as to what might be called a "routine purpose." A bureaucrat might be tempted to include a "nonroutine" use in the definition of "routine" and subvert the safeguards set up for individual privacy in this bill.

Therefore, the purpose of these amendments is to subject the agency determination to public scrutiny by providing 30 days for interested parties to submit to the agency after publication in the Federal Register written data, views, or arguments as to its interpretation of "routine purpose." I believe that this amendment strengthens the bill against potential bureaucratic abuses and urge that it be adopted.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from Illinois.

Mr. ERLENBORN. Mr. Chairman, I thank the gentleman for yielding to me. I want to say that the gentleman from Pennsylvania has furnished me with a copy of the amendments, and I support the amendments.

The CHAIRMAN. The question is on the amendments offered by the gentleman from Pennsylvania (Mr. Moorhead).

The amendments were agreed to.

AMENDMENT OFFERED BY MR. MOORHEAD OF PENNSYLVANIA

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I offer a technical amendment.

The Clerk read as follows:

Amendment offered by Mr. Moorhead of Pennsylvania: On page 33, line 2, after "(F)" insert "and (i)".

On page 30, line 24, strike "(j) or".

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I will be brief in explaining this amendment, which has been previously discussed with the minority side. Very simply, it tightens up a part of the bill where a loophole might exist. It provides that if the head of an agency utilizes the authority under subsection (j) of the bill to exempt a system of records from this law, such action shall not exempt the particular agency from safeguards to the public against abuse of such exemption authority as provided in subsection (i), imposing criminal penalties for violations of the act.

I trust that the amendment will be adopted.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from Illinois.

Mr. ERLENBORN. Mr. Chairman, I thank the gentleman for yielding to me. I do support the amendment.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Pennsylvania (Mr. Moorhead).

The amendment was agreed to.

AMENDMENT OFFERED BY MR. ERLENBORN

Mr. ERLENBORN. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Erlenborn: On page 34, in line 14, strike out the word "or";

In line 16, strike out the period and insert in its place a semi-colon; and

After line 16, insert the following:

"(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

"(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

"(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence."

Mr. ERLENBORN (during the reading). Mr. Chairman, I ask unanimous consent that further reading of the amendment be dispensed with and that the amendment be printed in the Record at this point.

The CHAIRMAN. Is there objection to the request of the gentleman from Illinois?

There was no objection.

(Mr. Erlenborn asked and was given permission to revise and extend his remarks.)

Mr. ERLENBORN. Mr. Chairman, a copy of this amendment has been furnished to the majority, and since the amendment has not been read, I would like to briefly describe its three purposes. This adds in the specific exemption, subsection (k)(3) exemptions not found in the bill.

The first is investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualification for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of the source that was a confidential source, promised confidentiality.

As I said during the general debate, the Washington Post this morning, in an editorial, incorrectly described this as closing the files entirely. The files will be open. The individual will have access to the files and to the information contained therein. But we will protect the confidentiality of statements that have been given in the past on a promise of confidentiality, express or implied, and will protect in the future the confidentiality of statements that were given by someone with an express promise of confidentiality.

The second part of the amendment will exempt testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process.

This amendment has been requested by the Civil Service Commission. Under the bill, without this exemption, each test that is given—and there are hundreds of such tests that have been prepared by the Civil Service Commission—would be available to any individual who took the test—the questions and the answers. That test then would be

compromised and could never be used again. The Civil Service Commission would have to prepare a whole new test the next time a test in that area was given. This would be an unnecessary expense without enhancing the privacy of any individual. I think this portion of the amendment is certainly warranted.

Lastly, my amendment provides a specific exemption for evaluation material used to determine potential for promotion in the Armed Services, but again, only to the extent that it is necessary to protect a confidential source.

As to the first and third portions of this amendment, the protection of confidential sources, I think it is very interesting that the House today overrode a veto of amendments to the Freedom of Information Act, and that Freedom of Information Act gets into the same area of information.

Listen to the report of the conference committee relative to the Freedom of Information Act. It says:

> In every case where the investigatory records sought were compiled for law enforcement purposes, either civil or criminal in nature, the agencies can withhold the names, addresses and other information that would reveal the identity of a confidential source who furnished the information.

So there, in that act, we saw the need to protect the confidential source. I think we should do likewise in this act.

Mr. Chairman, the President on October 9th issued a statement endorsing the legislation before us. He had in that statement, however, one reservation. He said:

> H.R. 16373, the Privacy Act of 1974, has my enthusiastic support except for the provisions which will allow unlimited individual access to records vital to determining eligibility and promotion in the Federal service and access to classified information.

I strongly urge a floor amendment permitting workable exemptions to accommodate these situations. This is the amendment that will meet the President's concern, and I think it is a valid concern.

There is one last observation that I would like to make. I have here a copy of the decision in the case of Koch against the Department of Justice. It is a decision of the District Court of the District of Columbia, which is considered one of the more liberal courts, and the judge was Judge Gerhard Gesell, who is considered one of the more liberal judges.

I would like to read just one or two excerpts from the decision.

The judge says:

> Background files on Congressman Bingham which were compiled during investigations into his eligibility for certain high Government posts. Such employment checks are routine, fully authorized, and essential to the maintenance of integrity in government service.

The court later in another part says as follows:

> Plaintiffs' narrower interpretation of that exemption is unjustified, since it would require disclosure of highly confidential information supplied to Bureau investigators. In order to insure such confidentiality, FBI files may be withheld if law enforcement was a significant aspect of the investigation.

The judge goes on further to say:

This is true even if the laws being enforced were regulatory rather than criminal in nature.

Then the judge later says:

Even inactive investigatory files may have to be kept confidential in order to convince citizens that they may safely confide in law enforcement officials.

Mr. Chairman, unless we adopt this amendment, confidential statements given to investigators in the past will be made available to the persons about whom the investigations are being made.

The CHAIRMAN. The time of the gentleman from Illinois (Mr. Erlenborn) has expired.

(By unanimous consent, Mr. Erlenborn was allowed to proceed for 2 additional minutes.)

Mr. ERLENBORN. Mr. Chairman, there are literally hundreds of thousands of people across this country, many Members of Congress included, who in the past have given confidential statements relative to people who are being considered for high Government posts. These confidential statements will be opened up to the individual who is being investigated if the bill passes without amendment—and, I think equally important, in the future we would not be able to conduct meaningful investigations into such matters as the appointment of a Vice President and the appointment of members of the courts, including the Supreme Court, District Courts, and so forth, unless we have limited ability to promise confidentiality where it is necessary to get candid information concerning individuals.

Mr. Chairman, I hope that my amendment will be supported.

Mr. SMITH of New York. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I yield briefly to the gentleman from New York.

Mr. SMITH of New York. Mr. Chairman, do I understand that the gentleman's amendment would open the files, as far as the background statements themselves are concerned, as long as the identity of the person making those statements was preserved?

Mr. ERLENBORN. Mr. Chairman, I thank the gentleman for his question. The gentleman is exactly right.

The information, derogatory or otherwise, will be made available to the individual. The only portion that will be kept confidential is the name of the one who has given the information in confidence, or such information as might lead to his identity.

Mr. SMITH of New York. I thank the gentleman.

Mr. HOLIFIELD. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I yield to the gentleman from California.

Mr. HOLIFIELD. Mr. Chairman, I would like, of course, to say, not being a lawyer, that I find myself at somewhat of a disadvantage, with the very complexity of this bill.

I recognize the laudable purpose of it. I do intend to vote for the bill. In committee I did vote with the gentleman for this amendment, or one very close to it. There seems to be a difference of opinion as to whether this is the exact amendment or not. I expect to vote for it at this time.

I think that if we do reveal the sources of confidential information, after we have or an agency has obtained the information under the promise of protecting the source, it would imperil the access to information which we should have.

The CHAIRMAN. The time of the gentleman from Illinois (Mr. Erlenborn) has expired.

(On request of Mr. Holifield and by unanimous consent, Mr. Erlenborn was allowed to proceed for 2 additional minutes.)

Mr. HOLIFIELD. Mr. Chairman, I also believe that there might be a great danger, both to the Government and to the individual involved who gave that information, if the source was revealed.

Therefore, I find myself in general agreement with this amendment. I voted for the amendment in committee, although we lost it in committee, as the gentleman remembers. It does seem to me that it is a protective amendment.

We are skating on thin ice, between freedom of information and privacy of information, and I think the extra care that this would give or the extra protection it would give to sources that might be vital to the Government in many fields is worthy of consideration.

Mr. Chairman, I would hope that the chairman of the subcommittee, unless there is a very strong reason, which he will undoubtedly express if there is such a reason, might be able to accept this amendment.

Mr. ERLENBORN. Mr. Chairman, I thank the gentleman for his support.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I will say to the chairman of the full committee that I felt that I am bound by the vote of the full committee, which, as I recall, was 22 to 11 not to accept the amendment offered by the gentleman from Illinois.

I have tried to negotiate portions of this matter with him, but unsuccessfully, even though we have been very successful in reaching agreements on many other pieces of legislation.

Mr. GOLDWATER. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I will be happy to yield to the gentleman from California.

Mr. GOLDWATER. I thank the gentleman for yielding. I would like to ask him a question. I can appreciate what the gentleman is trying to do, and that is to protect the parties' sources of information, but is there anywhere any protection to eliminate the inclusion of vicious rumors, subjective opinions, false statements, or honest mistakes that are in the records that are supplied by these parties?

Mr. ERLENBORN. Yes. I would point out that the information in the file will be made available quite generally, whether it is derogatory, defamatory, or whatever. We will only protect the confidential source.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I make the point of order that a quorum is not present.

The CHAIRMAN. The Chair will count.

Thirty-six Members are present, evidently not a quorum.

In view of the inoperability of the electronic device, the Clerk will call the roll.

The Clerk called the roll, and the following Members failed to answer to their names:

[Roll No. 636]

Ashley	Fraser	Parris
Baker	Fulton	Patman
Bergland	Gibbons	Pike
Bingham	Ginn	Poage
Blatnik	Goodling	Podell
Boggs	Grasso	Quie
Brasco	Gray	Rarick
Breaux	Green, Oreg.	Reid
Broomfield	Hanrahan	Riegle
Brotzman	Hansen, Wash.	Roncallo, N.Y.
Burton, John	Hébert	Rooney, N.Y.
Burton, Phillip	Heckler, Mass.	Rosenthal
Camp	Jarman	Runnels
Carey, N.Y.	Jones, Ala.	Sandman
Chappell	Jones, N.C.	Shoup
Clay	Kuykendall	Stark
Cohen	Leggett	Steele
Conable	Luken	Steiger, Ariz.
Conlan	McEwen	Teague
Coughlin	McKinney	Tiernan
Cronin	Madigan	Ullman
Davis, Ga.	Martin, Nebr.	Veysey
Diggs	Mathias, Calif.	Waldie
Dingell	Mayne	Wilson, Charles H., Calif.
Downing	Meicher	Wyatt
Drinan	Mitchell, Md.	Wyman
Esch	Murphy, Ill.	Young, Alaska
Eshleman	Murphy, N.Y.	Zion
Evans, Colo.	Nichols	
Foley	Obey	
Ford	O'Hara	

Accordingly the Committee rose; and the Speaker pro tempore (Mr. McFall) having assumed the chair, Mr. Brademas, Chairman of the Committee of the Whole House on the State of the Union, reported that that Committee, having had under consideration the bill H.R. 16373, and finding itself without a quorum, he had directed the roll to be called, when 344 Members responded to their names, a quorum, and he submitted herewith the names of the absentees to be spread upon the Journal.

The Committee resumed its sitting.

The CHAIRMAN. The Chair recognizes the gentleman from Pennsylvania (Mr. Moorehead).

Mr. MOOREHEAD of Pennsylvania. Mr. Chairman, I rise in opposition to the amendment.

I oppose the amendment because I think it makes second-class citizens out of some 4½ million Government employees, civil and military. And I wish to report to the membership that the amendment is opposed by the Government Employees Council, AFL-CIO.

Mr. FASCELL. Mr. Chairman, will the gentleman yield?

Mr. MOOREHEAD of Pennsylvania. At this time I yield to my colleague on the committee, the gentleman from Florida (Mr. Fascell).

Mr. FASCELL. Mr. Chairman, I thank the gentleman for yielding.

I also am strongly opposed to this amendment, because what it does is set up a whole new exemption and write a provision into law which does not now exist. Otherwise there would be no reason for the amendment.

The amendment specifically exempts from the provisions of this bill identity or source of information. There is no such exemption now in the law.

Other Members, just as I have been, have been asked many, many times to give information. Never have I had any Government agency or agent say to me, "Sir, the information you give me is classified" or "The information will be kept confidential."

Mr. Chairman, what the pending amendment would do is write this tremendous loophole into the statutes of this country and change the complete thrust of this bill. That is what this amendment does, is to give the applicant the right to look at information; the burden is then on him to prove his innocence without ever knowing who the person was or what the source was of the adverse or derogatory information.

Mr. Chairman, this amendment destroys the principal purpose of this bill.

Ms. ABZUG. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentlewoman from New York.

Ms. ABZUG. Mr. Chairman, I might add that should there be any serious question of the need to protect the confidentiality of informants' identity for law enforcement activities or for national security purposes, that identity would be protected under specific exemptions in the bill which we have before us.

So that the only purpose that the amendment offered by the gentleman from Illinois (Mr. Erlenborn) would serve would be, as has been stated by both of my colleagues on the committee, to exempt millions of civilian employees and military employees from the safeguard provisions of this bill, which are so desperately needed. The need for privacy protections for these particular groups has been amply documented by a GAO report which is in our committee and which the gentleman is well aware of.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, in the interest of brevity, I yield back the balance of my time and I hope that a vote can be called for promptly.

Mr. GOLDWATER. Mr. Chairman, I move to strike the last word.

Mr. Chairman, I rise with certain reservations with regard to this amendment. I likewise am greatly concerned with protecting the rights of applicants for civil service employment and with insuring that the applicant have access to information about him that is furnished by third parties. I likewise recognize the difficult question regarding policy matters contained in this particular bill, in that, if taken in its true sense, open up disclosure of third-party information.

I would like at this point to ask the author of the amendment (Mr. Erlenborn) a few questions if he would be kind enough to respond.

Mr. Erlenborn, what in this provision provides for the applicant to rebut or to countermand any vicious rumors or subjective opinions or false statements or honest mistakes taken from third parties about an individual?

Mr. Erlenborn. If the gentleman will yield, the bill itself provides for the first time the right of access by an individual to records maintained concerning himself or herself, and the bill provides that if the individual believes that the information is inaccurate, he has a right to demand that the information be corrected. This is as to all records generally and can be applicable to these free employment and security investigation files as well. Therefore, the application of the bill—not the amendment—but the application of the bill is such that it provides this right to the individual to demand that a file be made accurate if he considers it to be inaccurate.

Mr. Goldwater. How will the applicant know that there is included in his file information from a third party or confidential source?

Mr. Erlenborn. Will the gentleman yield?

Mr. Goldwater. Yes, I yield to the gentleman.

Mr. Erlenborn. As provided in my amendment, the information contained in the file will be made available to the individual about whom the file has been maintained.

Only to the extent that the confidential source would be compromised would we keep the name of the individual who is the confidential source or such information as would identify him from the applicant. That information would be kept from the individual seeking information. Otherwise, all the rest of the contents of the file, including any of this derogatory information, would be made available to the jobseeker.

Mr. Goldwater. Is it your understanding that your amendment notwithstanding, the applicant would be allowed to file with this information obtained from a confidential source his own version or his own rebuttal or perhaps his own denial of that accusation or erroneous information?

Mr. Erlenborn. Yes. Under the terms of the bill itself, that would be a remedy available to the individual about whom the file was kept.

Mr. Goldwater. One other question: It is my understanding that promises of confidentiality have in most cases only been made on the strength of bureaucratic authority as to most Civil Service records and that there is no statutory authority for agencies to grant confidentiality or protection; am I correct?

Mr. Erlenborn. If the gentleman will yield, in the past, of course, an individual never had an opportunity to go into his security clearance file or into his free employment file.

Therefore, the question really never arose.

In the past there has been lawfully expressed and implied promises of confidentiality given to those who have made statements to investigators.

The function of this bill, if it is not amended by the Erlenborn amendment, will be to open up all of those old files so that those state-

ments that were given in confidence will now be made available to the individual.

The gentleman from Florida says that he has never had any promises, express or implied. In that case, his name will be made available if he is one who has given such a statement, because the only thing that would be protected are those confidential sources.

Mr. GOLDWATER. Obviously, it appears by this language in the amendment that we are in essence legitimatizing this practice.

The CHAIRMAN. The time of the gentleman from California has expired.

(By unanimous consent, Mr. Goldwater was allowed to proceed for 1 additional minute.)

Mr. GOLDWATER. One last question, Mr. Chairman, and that is: This gives discretion to the agency to arbitrarily decide which information it will supply, and which information it will withhold. The question that occurs to me is, where is the check and balance? It is the intention of this committee that information should be disclosed to an applicant or to an individual upon request, but, if there is this discretion within the agency, then where is the check and the balance? Where is the impartial review, the in camera inspection to determine whether in fact all information is included, or whether in fact third parties should perhaps be made available?

Mr. ERLENBORN. If the gentleman will again yield, I think the general access to the courts, as we provide in the bill, would provide that. However, let me make this one additional point, and that is that many Members of this House, myself not included, but many Members of the House have sponsored the newsmen's shield bill, realizing the great advantage that there is in confidential sources, and it will protect such sources of newsmen and newspapers, and it would shield them so that they would not have to reveal their sources and, if we pass that legislation we would find that possibly just wild rumors could be printed in the paper, and the source of the information to the news media could not be revealed.

The CHAIRMAN. The time of the gentleman has again expired.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I ask unanimous consent that all debate on this amendment and all amendments thereto do now close.

The CHAIRMAN. Is there objection to the request of the gentleman from Pennsylvania?

There was no objection.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Illinois (Mr. Erlenborn).

The question was taken, and the Chairman announced that the noes appeared to have it.

RECORDED VOTE

Mr. ERLENBORN. Mr. Chairman, I demand a recorded vote.

A recorded vote was ordered.

The vote was taken by clerks, and there were—ayes 192, noes 177, not voting 65, as follows:

[Roll No. 637]

AYES—192

Abdnor
Anderson, Ill.
Andrews, N. Dak.
Archer
Arends
Armstrong
Ashbrook
Bauman
Beard
Bell
Bevill
Biester
Blackburn
Bray
Breaux
Brinkley
Brotzman
Brown, Mich.
Brown, Ohio
Broyhill, N.C.
Broyhill, Va.
Burgener
Burke, Fla.
Burleson, Tex.
Butler
Byron
Carter
Casey, Tex.
Clancy
Clausen, Don H.
Clawson, Del.
Cleveland
Collier
Collins, Tex.
Conte
Coughlin
Crane
Daniel, Dan
Daniel, Robert W., Jr.
Davis, S.C.
Dellenback
Denholm
Dennis
Derwinski
Devine
Dickinson
Downing
Duncan
du Pont
Edwards, Ala.
Erlenborn
Esch
Findley
Fish
Fisher
Flowers
Flynt
Forsythe
Fountain
Frelinghuysen
Frenzel
Frey
Fuqua
Gettys
Ginn
Goodling
Gray
Gross
Grover
Gubser
Gude
Guyer
Hammerschmidt
Hansen, Idaho
Hastings
Hays
Heckler, Mass.
Heinz
Henderson
Hillis
Hinshaw
Hogan
Holifield
Holt
Horton
Hosmer
Huber
Hunt
Hutchinson
Ichord
Jarman
Johnson, Colo.
Johnson, Pa.
Jones, Okla.
Jones, Tenn.
Jordan
Kemp
Ketchum
Lagomarsino
Landgrebe
Latta
Lent
Lott
Lujan
McClory
McCloskey
McCollister
McDade
McEwen
McKay
Mahon
Mallary
Mann
Maraziti
Martin, Nebr.
Martin, N.C.
Mayne
Milford
Miller
Minshall, Ohio
Mizell
Molohan
Moorhead, Calif.
Myers
Nedzi
Nelson
O'Brien
Patten
Pettis
Pike
Powell, Ohio
Preyer
Price, Tex.
Pritchard
Quie
Quillen
Randall
Regula
Rhodes
Roberts
Robinson, Va.
Robison, N.Y.
Rousselot
Ruppe
Satterfield
Scherle
Schneebeli
Sebelius
Shriver
Shuster
Sikes
Skubitz
Smith, N.Y.
Snyder
Spence
Stanton, J. William
Steed
Steele
Steiger, Ariz.
Steiger, Wis.
Stratton
Stubblefield
Symms
Talcott
Taylor, Mo.
Taylor, N.C.
Thomson, Wis.
Thone
Treen
Ullman
Vander Jagt
Veysey
Waggonner
Walsh
Wampler
Ware
Whalen
White
Whitehurst
Widnall
Wiggins
Williams
Wilson, Bob
Winn
Wydler
Wylie
Young, Alaska
Young, Fla.
Young, Ill.
Young, S.C.
Zion
Zwach

NOES—177

Abzug
Adams
Addabbo
Alexander
Anderson, Calif.
Andrews, N.C.
Annunzio
Ashley
Aspin
Badillo
Bafalis
Barrett
Bennett
Biaggi
Bingham
Boland
Bolling
Bowen
Brademas
Breckinridge
Brooks
Brown, Calif.
Buchanan
Burke, Calif.
Burke, Mass.
Burlison, Mo.
Burton, John
Burton, Phillip
Carney, Ohio
Chisholm
Clay
Collins, Ill.
Conyers
Corman
Cotter
Culver
Daniels, Dominick V.
Danielson
de la Garza
Delaney
Dellums
Dent
Diggs
Dingell
Donohue
Dorn
Drinan
Eckhardt
Edwards, Calif.
Ellberg
Evans, Colo.
Evins, Tenn.
Fascell
Flood
Foley
Ford
Fraser
Gaydos
Giaimo.
Gibbons
Gilman
Goldwater
Gonzalez
Green, Pa.
Gunter
Haley
Hamilton
Hanley
Hanrahan
Hansen, Wash.
Harrington
Hawkins
Hechler, W. Va.
Helstoski
Hicks
Holtzman
Howard
Hudnut
Hungate
Johnson, Calif.
Karth
Kastenmeier
Kazen
Kluczynski
Koch
Kyros
Leggett
Lehman
Litton
Long, La.
Long, Md.
Luken
McCormack
McFall
McSpadden
Macdonald
Madden
Matsunaga
Mazzoli
Meeds
Melcher
Metcalfe
Mezvinsky
Mills
Minish
Mink
Mitchell, N.Y.
Moakley
Montgomery
Moorhead, Pa.
Morgan
Mosher
Moss
Murphy, N.Y.
Murtha
Natcher
Nix
Obey
O'Hara
Owens
Passman
Pepper
Perkins
Peyser
Pickle
Price, Ill.
Rangel
Rees
Reid
Reuss
Rinaldo
Rodino
Roe
Rogers
Roncalio, Wyo.
Rooney, Pa.
Rose
Rosenthal
Rostenkowski
Roush
Roy
Roybal
Ryan
St Germain
Sarasin
Sarbanes
Schroeder
Seiberling
Shipley
Sisk
Slack
Smith, Iowa
Stanton, James V.
Stark
Steelman
Stephens
Stokes
Studds
Sullivan
Symington
Thompson, N.J.
Tiernan
Traxler
Udall
Van Deerlin
Vander Veen
Vanik
Vigorito
Whitten
Wilson, Charles, Tex.
Wolff
Wright
Yates
Yatron
Young, Ga.
Young, Tex.
Zablocki

NOT VOTING—65

Baker	Fulton	Patman
Bergland	Grasso	Poage
Blatnik	Green, Oreg.	Podell
Boggs	Griffiths	Railsback
Brasco	Hanna	Rarick
Broomfield	Harsha	Riegle
Camp	Hébert	Roncallo, N.Y.
Carey, N.Y.	Jones, Ala.	Rooney, N.Y.
Cederberg	Jones, N.C.	Runnels
Chamberlain	King	Ruth
Chappell	Kuykendall	Sandman
Clark	Landrum	Shoup
Cochran	McKinney	Staggers
Cohen	Madigan	Stuckey
Conable	Mathias, Calif.	Teague
Conlan	Mathis, Ga.	Thornton
Cronin	Michel	Towell, Nev.
Davis, Ga.	Mitchell, Md.	Waldie
Davis, Wis.	Murphy, Ill.	Wilson, Charles H., Calif.
Dulski	Nichols	
Eshleman	O'Neill	Wyatt
Froehlich	Parris	Wyman

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I rise to see if I can determine how many more amendments there are expected to be offered, to see if it would be possible to arrive at an agreement on time for closing debate on this legislation.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from Illinois.

Mr. ERLENBORN. Mr. Chairman, we just checked at the minority desk as to how many amendments we are aware of. There are about 12 or 13, not all of them are contested; probably 4 or 5 are contested.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I will not make my unanimous consent request at this point.

AMENDMENT OFFERED BY MR. FASCELL

Mr. FASCELL. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. FASCELL: Page 31, line 5, strike out line 5 and all that follows through line 13 and insert in lieu thereof the following:

"(3) In any suit brought under the provisions of subsection (g)(1)(B) or (C) of this section in which the court determines—

"(A) that the agency has refused or failed to comply with any of the provisions of this section, or any rule promulgated thereunder, the United States shall be liable to the individual in an amount equal to the sum of—

"(i) actual damages sustained by the individual as a result of the refusal or failure; and

"(ii) the costs of the action together with reasonable attorney fees as determined by the court; or

"(B) that the agency's refusal or failure has been willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—

"(i) actual damages sustained by the individual as a result of the refusal or failure; and

"(ii) punitive damages allowed by the court; and

"(iii) the costs of the action together with reasonable attorney fees as determined by the court."

(Mr. Fascell asked and was given permission to revise and extend his remarks.)

Mr. FASCELL. Mr. Chairman, what my amendment does is to restore to the bill language which was in the bill in subcommittee, stricken out in the full committee, dealing with damages, the right of damages and remedies available to the individual.

If the members of the committee will follow me, in the present bill on page 31 with the section we are talking about, they will find the remedies in the lawsuit there for actual damages sustained by the individual, together with the court costs and reasonable attorney fees.

The Members will notice, however, that it is predicated only in those cases where there is willful, arbitrary or capricious action by the agency. There, the Members will find a complete departure from ordinarily understood law, tort law. A remedy that would be available to an individual if he were damaged in this case, we limit his recovery to actual damages. We require him to prove that he was damaged by a willful, arbitrary, or capricious violation, the kind of burden which is a very difficult burden, I assure the Members, as a lawyer. The Members who are lawyers know that, where we place that kind of a burden only in those cases where we seek punitive damages.

So, what my amendment would do would be to restore the right of actual damage in those cases where there is a refusal or a failure to comply with the law, aside from whether it is willful, capricious or arbitrary; just sheer negligence, whether it is inadvertent or not. The fact that there is a refusal or an inability or a failure to comply with the law then will allow the individual to redress for actual damages and the costs of the action.

Then, what we do in those cases where we have willful, arbitrary or capricious action by an agency is to allow recovery for actual damage or punitive damage. So, what this amendment does, to recap, is to take the reasonable remedy, restore the rights to the individual who is actually damaged in the cases where, in the present bill now, it is only actual damages in cases of willful, arbitrary or capricious action. My amendment would give the person the right to recover actual damages in cases where there is a failure to comply with the law. It would also give him punitive damages in those cases where there is willful, arbitrary or capricious action by the agency.

Mr. BUTLER. Mr. Chairman, will the gentleman yield for a question?

Mr. FASCELL. Yes.

Mr. BUTLER. My understanding is that, in effect, what you are providing for are punitive damages in case of willful, arbitrary, or capricious action of the United States in withholding information?

Mr. FASCELL. The gentleman is correct. That is one part of the amendment.

Mr. BUTLER. Can the gentleman cite me a precedent in the statutes in the United States, or has the United States adopted a law holding itself open for willful punitive damages? Can the gentleman cite me a statute where any nation of the world has held itself open for punitive damages in the statute?

Mr. FASCELL. Frankly, I do not have that citation. But the gentleman knows where one has a willful, capricious, arbitrary action by the Government, and one is trying to protect the rights of the individual, mine or the gentleman's, it seems to me that leaving it to the court to decide whether or not there ought to be punitive damages under our system—I am perfectly willing to leave it to the system. We do it in all kinds of cases with respect to the individual redress against the Government of the United States.

Mr. BUTLER. May I fairly observe there is no sovereignty in the world that exposes itself to punitive damages by a statute of this nature?

Mr. FASCELL. I thank the gentleman for his observation.

Mr. MCCLOSKEY. Mr. Chairman, will the gentleman yield?

Mr. FASCELL. I yield to the gentleman from California.

Mr. MCCLOSKEY. I thank the gentleman for yielding. I think we have made an exhaustive study of the statutes of this Nation, and if we are to adopt by this amendment punitive damages, it would be the first time in history that the United States has made itself subject to punitive damages for any cause or in any case. We have adopted six or seven provisions by statute to impose attorney's fees against the United States, but this would be the first time for punitive damages.

I would like to ask the gentleman in the well, is it not true that there would be no way of ascertaining in advance of any one year, when this Congress is ascertaining the budget, what might possibly be the amount of damages that might be awarded?

Mr. FASCELL. The gentleman is absolutely correct. And we have the same problem in respect to awards made in condemnation cases. We have the same problem.

Mr. MCCLOSKEY. Mr. Chairman, I move to strike the requisite number of words.

Mr. Chairman, I would like to speak against this amendment, and I would like to call the attention of my colleagues to the very real problem that the amendment imposes on a government servant. We have just overridden a presidential veto of the Freedom of Information Act, and we have put in that statute extremely strong and rigorous provisions, penalizing a Government agency and an employee who may improperly withhold information from the public or from the Congress or from other Federal employees. We have wanted to penetrate the veil of secrecy which Government agencies and Government bureaucrats have been accustomed to throw around the protection of information.

If we enact this amendment, however, we will, in effect, be placing upon the Government bureaucrat the choice that if he reveals information improperly, he may subject his agency to punitive damages. If he withholds the information, on the other hand, he is subject only to ordinary damages, attorneys' fees, and costs.

Government employees, faced with that choice, faced with the imposition of punitive damages if they improperly release information, as against only attorneys' fees and costs if they improperly withhold will be tempted to withhold. We thus endanger that great principle which we have just established when we overrode the presidential veto of the Freedom of Information Act Amendments.

Mr. FASCELL. Will the gentleman yield?

Mr. McCLOSKEY. I yield to the gentleman.

Mr. FASCELL. Let us talk about my problem. You are a Government employee and I want some information from you, is there any hardship on you or any burden to make that information available to me?

Mr. McCLOSKEY. I may violate the Freedom of Information Act if I do not reveal it. Yet I may be subject to punitive damages if I do.

Mr. FASCELL. No, the punitive damage language only says, "willful, capricious, or arbitrary."

Mr. McCLOSKEY. Mr. Chairman, I do not think any of us who have practiced law would care to stake our future and our future careers on what some court might determine to be "willful, capricious, and arbitrary."

Mr. FASCELL. Mr. Chairman, will the gentleman yield further?

Mr. McCLOSKEY. Certainly.

Mr. FASCELL. Then I would suggest to the gentleman that he should make the information completely available to them.

Mr. ECKHARDT. Mr. Chairman, will the gentleman yield?

Mr. McCLOSKEY. I yield to the gentleman from Texas.

Mr. ECKHARDT. Mr. Chairman, the gentleman has spoken of the term "willful, arbitrary, and capricious."

Can the gentleman give me any reason in the world why I, as a person who has been injured, should not recover actual damages from a dumb but ineffective bureaucrat, since I can get them from one who acts willfully?

One can be hurt just as badly by a dumb, well intentioned person as one can by an intelligent, conniving one, can he not?

Mr. McCLOSKEY. Mr. Chairman, let me respond to the gentleman in this way: that we are trying to balance two great interests here. We are trying to balance the necessity of balancing the budget, and we are trying to protect the Government from undue liability.

I think it is wrong to make the Government of the United States and this congressional budget subject to an absolutely incalculable amount of liquidated damages. If we had a hundred lawsuits, and if we had a hundred verdicts of $1 million each, there would be no guarantee in any way that this Congress could protect itself against that liability. It seems to me, when we balance the rights of the individual against the Government, that to add punitive damages and to set this kind of a precedent is an unfortunate mistake. It would be the first time in history this has occurred.

This would be singling out invasion of privacy as a particular right of an individual against the Government, a right that would weigh heavier than all other rights.

We have just seen a Presidential veto sustained in the case of an individual who could not recover damages against the Government in an ordinary lawsuit. Why should we make invasion of privacy a special right with this extraordinary remedy?

Mr. ECKHARDT. Mr. Chairman, will the gentleman yield further?

Mr. McCLOSKEY. I yield to the gentleman from Texas.

Mr. ECKHARDT. Mr. Chairman, aside from the point the gentleman is making with respect to punitive damages, the question I am raising is that this amendment is the only vehicle that would correct the situation, because actual damages are not available to an injured party because the person who hurt him did not do so intentionally.

Is that not what the gentleman reads in the original language, and is that not corrected by the amendment?

Mr. McCLOSKEY. Mr. Chairman, I do not believe that the individual is denied actual damages if he can prove them. In cases of this kind, of course, it is quite often difficult to prove actual damages, but that is not necessarily a reason to establish the extraordinary remedy of punitive damages.

Mr. ECKHARDT. Mr. Chairman, I move to strike the requisite number of words, and I rise in support of the amendment.

Mr. Chairman, I wish to speak only briefly. I simply wish to point out, if I understand the amendment correctly, the thrust of the first part of the amendment is to avoid what seems to me to be a terrible error in the bill, and that is this: that a person who is injured by virtue of a mistake unintentionally made by a bureaucrat has no redress for that injury.

Will the author of the amendment inform me whether I am correct on that?

Mr. FASCELL. Mr. Chairman, will the gentleman yield?

Mr. ECKHARDT. I yield to the gentleman from Florida.

Mr. FASCELL. Mr. Chairman, the gentleman from Texas is absolutely correct.

That provision is totally lacking in the bill, and that is what this amendment provides.

If the gentleman will yield further, I would like to respond to some of the remarks made by the gentleman from California. The gentleman said that we would not know how much money this would cost and that there is no way to budget it. That is the same problem the Government is faced with in all claims bills. We do not at any time know how much money it will cost and how much should be budgeted. Of course, I feel after today that we may never pass any again, but nevertheless we are stuck with the same problem in that respect.

It seems to me that this matter can be spelled out in a differnt way. We would force these individuals to file private claims bills. After numerous bills were filed and after they tried to get redress, we would force these people to take action. As the gentleman from Texas has said, this should be a matter of legal right, and they should have the right to collect damages.

Mr. ECKHARDT. Mr. Chairman, it also seems to me that the fears concerning punitive damages are ill-founded. The court must agree in these situations that they should be granted. I feel that the courts would seldom grant them against the United States if the United States was acting properly.

Mr. FASCELL. The gentleman is absolutely correct.

Mr. ERLENBORN. Mr. Chairman, I move to strike the requisite number of words, and I rise in opposition to the amendment.

(Mr. ERLENBORN asked and was given permission to revise and extend his remarks.)

Mr. ERLENBORN. Mr. Chairman, I know that the erudite gentleman from Texas (Mr. Eckhardt) is a lawyer. I have heard the gentleman discourse very learnedly on the floor of the House before. I understand the gentleman from Florida (Mr. Fascell) also has legal training.

As I believe most of the lawyers here in the House know, it is a general principle of law that the Government, in exercising its governmental functions, is not liable.

In exercising the proprietary functions, the Government can be liable; but it would be, as has been pointed out by others debating this amendment, unprecedented to make Government liable for punitive damages, because there has been no precedent in the past for making any Government liable for punitive damages.

I would also like to point out that the bill, as it was being considered in committee, had a punitive damage section. The committee, in its wisdom, removed that by amendment before reporting the bill.

I hope the committee will be sustained on the floor and the amendment will be defeated.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I move to strike the requisite number of words.

Mr. Chairman, I regret that I cannot, as floor manager, accept this amendment, although as an individual Member I support it.

Permit me to explain my position. When the bill was reported by the subcommittee, it contained a punitive damages provision. However, this provision, by a close 18 to 14 vote in the full committee, was deleted.

Therefore, although I personally support the amendment, I do not feel, as floor manager, that I can argue in favor of the amendment.

Let me state to the Chair that after the action on this amendment, it is the intention of myself to move that the committee rise.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Florida (Mr. Fascell).

The amendment was rejected.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I move that the Committee do now rise.

The motion was agreed to.

Accordingly the Committee rose; and the Speaker having resumed the Chair, Mr. Brademas, Chairman of the Committee of the Whole House on the State of the Union, reported that that committee, having had under consideration the bill H.R. 16373 to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, had come to no resolution thereon.

[From the Congressional Record—House, Nov. 21, 1974]

HOUSE CONTINUES CONSIDERATION OF H.R. 16373 AND PASSES IT WITH AMENDMENTS

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I move that the House resolve itself into the Committee of the Whole House on the State of the Union for the further consideration of the bill (H.R. 16373) to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies.

The SPEAKER. The question is on the motion offered by the gentleman from Pennsylvania (Mr. Moorhead).

The motion was agreed to.

The SPEAKER. The Chair requests the gentleman from Tennessee (Mr. Fulton) to assume the Chair temporarily.

IN THE COMMITTEE OF THE WHOLE

Accordingly the House resolved itself into the Committee of the Whole House on the State of the Union for the further consideration of the bill H.R. 16373, with Mr. Fulton (Chairman pro tempore) in the chair.

The CHAIRMAN pro tempore. When the Committee rose on yesterday, the amendment in the nature of a substitute to the bill was subject to amendment at any point.

Are there further amendments?

AMENDMENT OFFERED BY MR. MOORHEAD OF PENNSYLVANIA

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Moorehead of Pennsylvania: On page 31, strike lines 5 through 9 and insert in lieu thereof the following:

"(3) In a suit brought under the provisions of subsection (g)(1) (B) or (C) of this section in which the court determines that the agency failed or refused to comply with any provision of subsection (g)(1) (B) or (C) of this section, the United States shall be liable to the individual in an amount equal to the sum of—"

(Mr. Moorhead of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, the purpose of this amendment is to insure that persons who are actually damaged by the failure of the Government agency to comply with the provisions of subsection (g)(1) (B) or (C) are compensated for their losses.

The amendment does not contain a provision for punitive damages, which was objected to yesterday. There is nothing in this amendment, therefore, which subjects the Government to an undue burden. The burden is on the citizen. The citizen must prove that there was a violation of the provision of this act. He must then prove that the adverse determination which damaged him was caused by the above violation. He must finally prove the damages caused by the violation.

With this substantial burden already placed on the litigant, I see no reason to require that proof also be offered of willful, arbitrary, or capricious action by the defendant agency.

This amendment was suggested as a reasonable compromise by the gentleman from Texas (Mr. Eckhardt), and I now yield to him.

Mr. ECKHARDT. Mr. Chairman, I thank the distinguished subcommittee chairman.

It will be recalled by those who heard the debate yesterday that the primary objection to the Fascell amendment was that the Government should not be subjected to punitive damages. I think that that was the major ground upon which that amendment was defeated.

Frankly, had I thought that the Government would practically be so jeopardized, I would have voted against it too. I did not think that it was a practical danger, but this amendment completely removes that proposition.

However, the amendment does afford a correction of what seemed to me to be a very bad defect in the existing language, and that is that even though a person may not be able to get a job because his record falsely indicated his having been discharged when he had, in fact resigned, if an agent of Government made an innocent mistake in failing to go through with the procedure provided in this bill and the person whose record was falsely stated lost a job and therefore lost the money that he would have made on that job, he could still not sue because he could not show that the action was willful, arbitrary, or capricious.

It seems to me to be a matter of basic justice to permit a person who is actually injured by some act of an agent of the Government which is in violation of this subsection to recover on ordinary bases, that is, by showing that the act was violated and that he sustained injury.

There is nothing in this that would provide for any damages beyond his actual out-of-pocket expenses because of the flaw.

Mr. ICHORD. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from Missouri.

Mr. ICHORD. Mr. Chairman, I would like to ask the gentleman from Texas (Mr. Eckhardt) as to what is the standard of conduct that would cause the Government to be liable? Would the Government be liable? I would ask the gentleman from Texas this question: If there was an innocent mistake made in violation of this bill, would the Government be liable?

Mr. ECKHARDT. I do not know what "innocent mistake" means. As the gentleman knows, the act provides that if I ask for information concerning what is in my record I am entitled to have it. Having received that, and finding something that is erroneous in that information, I may then submit the correction. The agency must then either correct or must file reasons why it does not correct it.

Let us assume, for instance, that the agency, after I request the information, misplaces my letter and does not send me the information and, in the meantime, I seek a position with another government agency, and I am denied employment on the grounds that I have been discharged, when in fact I was not discharged. I think I am entitled to recover even though the action of the governmental agency may not have been willful; it is just a question of determining what the fact was.

Mr. ICHORD. There would be an element of negligent conduct, or unreasonable conduct, would there not?

Mr. ECKHARDT. I think so: yes.

Mr. ERLENBORN. Mr. Chairman, I move to strike the requisite number of words, and I rise in opposition to the amendment.

(Mr. Erlenborn asked and was given permission to revise and extend his remarks.)

Mr. ERLENBORN. Mr. Chairman, I think the gentleman from Missouri (Mr. Ichord) has asked a very good question as to standards of conduct. There are no standards of conduct required under this amendment. This amendment would make the Government a guarantor of the accuracy of everything that it has in its files.

The amendment says that any suit brought under subsection (g)(1)(B), (C) of this section does not have to refer to any standards of

conduct. What do (g)(1) (B) and (C) require? (B) requires that the agency maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness.

Now, if there is any inadvertent inaccuracy in a government file, a suit could be filed under this amendment, and damages asked and recovered.

(C) says:

> . . . fails to comply with any other provision of this action, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency. . . .

Again, this provision prescribes no standard of conduct. If a Government agency inadvertently violated any rule—whether a mistake be inadvertent or willful—a suit could be brought under this amendment for damages. This exposes the Government to undue liability. It makes the Government the guarantor of every piece of information that it has in every one of its files. It is not even prospective; this would be retroactive—Government employees would have to go through and clean up all their files so that they would not expose themselves to such liability.

I am surprised that the gentleman from Pennsylvania would offer this amendment at the last minute, without any warning. This was not reported out by the committee. This was not supported by the committee. Even though the gentleman is the manager of the bill, the gentleman does this on his own, and I am sure that he would tell the Members that that is correct.

Mr. MOORHEAD of Pennsylvania. If the gentleman will yield, I would not like to leave the inference in the record that this is a committee amendment. It is an amendment that was proposed by the gentleman from Texas (Mr. Eckhardt) as a reasonable compromise between the bill language on page 31—"willful, arbitrary, or capricious." I feel this compromise is necessary since punitive damages are not authorized in this bill because of the defeat of the Fascell amendment yesterday.

This is just to try to make a citizen whole when the Government has damaged him.

Mr. ERLENBORN. I am afraid the gentleman has just gone much too far on this in making the Government liable.

I read yesterday a statement that the President firmly supports this bill with only one reservation, and that reservation was taken care of by the adoption of the amendment I offered yesterday. But I am telling the Members if we adopt this amendment, we would be exposing the Government to blanket liability as a guarantor of every piece of personal information in its files, and I, for one, would recommend to the President—as important as this bill might be—that he veto it. We just cannot afford to have that kind of liability, leaving the Government so exposed. I hope the amendment will be defeated.

Mr. ECKHARDT. Mr. Chairman, I move to strike the requisite number of words, and I rise in favor of the amendment.

I do not believe the gentleman's fears are justified. This amendment does not require that the Government be the guarantor of every fact determined. The Government need only comply with the standards set out in (g)(1) and (B) and (C). Certainly the Government ought

to assure fairness in any determination. Surely the Government ought to be fair, and if it is unfair, the matter should be reviewable in court. Certainly the Government should do the things that are required under the standards here. Certainly the Government should supply the material. Certainly the Government should give the reasons, if it refuses to correct an asserted error.

If the Government does all of those things and acts in compliance with the language of the bill, the Government is not subjected to any liability whatsoever. There is no requirement of an assurance that the Government be absolutely correct with respect to every fact which is listed in a person's record. The Government need only be fair, and it need only comply with the standards of the act.

Mr. BUTLER. Mr. Chairman, will the gentleman yield?

Mr. ECKHARDT. I yield to the gentleman from Virginia.

Mr. BUTLER. I thank the gentleman for yielding.

As I understand, in the proposed amendment there is an addition to the discretionary authority which is in the court to assess reasonable attorneys' fees where the plaintiff substantially prevails; is that correct? So this would provide for actual damages in those situations as a matter of right, knowing that the law has not been complied with. Is there a precedent in other legislation by this automatic assessment of actual damages by a citizen against the U.S. Government?

Mr. ECKHARDT. Yes, there are several. I do not have bills in which this comes to mind immediately, but I know that we have had several here recently out of the Committee on Interstate and Foreign Commerce. I believe there was a provision of that nature with respect to citizens' suits regarding the products safety bill. I am not absolutely sure of that.

Mr. BUTLER. Is the Federal Government obligated under the products safety bill?

Mr. ECKHARDT. No, no.

Mr. BUTLER. I am talking about the Federal Government. Is there a law saying that a citizen can recover damages when a minor clerk fails to perform his duties timely and completely, fairly accurately, and so forth? Is there a precedent for that?

Mr. ECKHARDT. I do not know whether there is or not, but I would answer the gentleman in this way. I would say that if the Federal Government acts in violation of its own statutory obligations, I can think of no agency that should be called upon more to pay attorneys' fees, because the public pays the Federal Government attorneys' fees.

Mr. BUTLER. We are plowing new ground, then.

Mr. MOORHEAD of Pennsylvania. If the gentleman will yield, when this was taken up yesterday, there was great argument that punitive damages had no precedent. I think that was one of the reasons that that amendment was defeated. But the inference is clearly left that there are other statutes under which actual damages can be awarded against the Government.

Mr. ECKHARDT. I might also say that we do not affect that portion of the bill. Attorneys' fees are provided in the bill, whether this amendment is passed or not. If the gentleman wishes to strike that, he might still do it by amendment, even if this amendment is agreed to.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Pennsylvania (Mr. Moorhead).

The question was taken; and the Chairman announced that the noes appeared to have it.

Mr. ECKHARDT. Mr. Chairman, I demand a recorded vote.

A recorded vote was refused.

So the amendment was rejected.

AMENDMENT OFFERED BY MR. ICHORD

Mr. ICHORD. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Ichord: Page 28, line 16, strike out the period after the word "maintained" and add the following: ": *Provided, however*, that the provisions of this paragraph shall not be deemed to prohibit the maintenance of any record of activity which is pertinent to and within the scope of a duly authorized law enforcement activity."

Mr. ICHORD. Mr. Chairman, as I pointed out in general debate this amendment can be described as a clarifying amendment. The managers of the bill have stated that they did not intend to do what I questioned they might be doing, and this language was worked out in cooperation with the managers of the bill. It is really to make certain that political and religious activities are not used as a cover for illegal or subversive activities.

In its present form paragraph (4) would prohibit any agency from maintaining any record concerning the "political or religious belief or activity" of any individual, unless "expressly authorized by statute" or by the individual. The use of the terms "expressly authorized by statute" would seem to indicate that unless the statute by specific terms—rather than by "implication"—authorized the agency to maintain such a record, maintenance would be prohibited, and that this would therefore have the effect of prohibiting the maintenance of records concerning Communist and other subversive organizations on the theory that they are engaged in "political" activities.

We may well recognize that the purpose of the provision is commendable and legitimate in prohibiting the disclosure of such records with respect to conventional political and religious beliefs and activities, but that it can be construed to cover activities which are properly within the scope of legitimate law enforcement. For example, the Communist Party and similar groups may claim that they are within the scope of the provision of this paragraph as a "political" activity. Similarly, certain sects within the Black Muslim movement, which are engaged in activities described by the Director of the FBI as endangering the internal security, may claim exemption as a "religious" belief.

It is the purpose of the amendment to make clear that such activities as are pertinent to, and within the scope of, duly authorized law enforement activities are not meant to be excluded by the broad terms of paragraph (4). It is simply a clarifying amendment, so that we obviate any necessity for litigation on the reach of the paragraph.

(Mr. Ichord asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. ICHORD. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I understand that this amendment should be construed in the light of the colloquy we had yesterday, that there was no intention to interfere with the first amendment rights of citizens.

Mr. ICHORD. I state emphatically to the gentleman from Pennsylvania that this amendment is not intended to hurt in any way the exercise of the first amendment rights.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I have no objection on this side of the aisle to the amendment.

Mr. ICHORD. Mr. Chairman, before yielding back the balance of my time, there is one further clarification that I would like to have from the gentleman from Pennsylvania as a matter of legislative history.

I state to the gentleman that I have expressed the concern that this measure might adversely affect the operations of the industrial security program or might even destroy the operation of the industrial security program. The gentleman from Pennsylvania and the gentleman from Illinois have assured me privately that this was not intended, but I do think we should have some legislative history.

How will the provisions of this bill affect the operation of the industrial security program?

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, if the gentleman will yield, the gentleman has raised an important question and I am pleased to explain its application. This bill would not disturb current procedures used in industrial security investigations, in the transfer of classified or unclassified information in such matters, in security clearances, or other related industrial security needs. Our subcommittee recently conducted hearings on the industrial security program as related to the security classification system, so that we are quite familiar with the program.

Subsection (e)(2)(D) on page 27 of the bill permits any agency, including an agency involved in industrial security activities, to publish in the Federal Register a notice for each system of records it maintains. This notice would list the "routine purpose" for which the records are used or are intended to be used. Thus, a Federal agency engaged in industrial security matters would state that one of the "routine purposes" for which information about an individual is collected and used for security clearances or other uses is to carry out its responsibilities under the industrial security program. It could then transfer, use or maintain information about individuals, or otherwise operate its industrial security program just as it has in the past. I trust that this explanation answers the gentleman's question.

I trust that this explanation satisfies the gentleman from Pennsylvania.

Mr. ICHORD. I thank the gentleman for his clarification.

I would also like to ask the gentleman from Illinois, is that his understanding or interpretation? The term "routine use" is rather ambiguous without further legislative clarification.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. ICHORD. I yield to the gentleman from Illinois.

Mr. ERLENBORN. I agree with the interpretation given the language by the gentleman from Pennsylvania. I think it will be the obligation of each agency which maintains such a system to list what the uses of the records in that system will be. The word "routine," then, while itself a little ambiguous, will be definitely clarified by publication in the Federal Register of what actual uses will be the routine uses to which each record is put.

Mr. ICHORD. Mr. Chairman, I thank the gentleman for his explanation. I move the adoption of the amendment.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Missouri (Mr. Ichord).

The amendment was agreed to.

AMENDMENT OFFERED BY MR. GUDE

Mr. GUDE. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. GUDE: On page 23, strike out lines 18 through 21 and insert in their place the following:

"(7) to a person who is actively engaged in saving the life of such individual, if upon such disclosure notification is transmitted to the last known address of such individual; or".

Mr. GUDE. Mr. Chairman, the purpose of this amendment is to clarify one item I believe to be ambiguous in intent. In restricting the circumstances under which information on individuals could be disclosed by Federal agencies, it was the intention of the committee to exclude information which would be vital to the health or safety of an individual. For example, if there had been an accident, and the attending doctor needed the victim's medical history before proceeding with treatment which might be necessary to save his life, we would not want the Federal Government to be forbidden to transmit that information, nor would we want to require a time consuming approval process which might result in the individual's death before the information could be provided.

However, I believe the current language of the bill is too vague in this regard, in that it would permit such disclosures without prior permission in less than emergency cases, and it does not make clear to whom the information could be discussed. My amendment would simply leave no doubt as to the intent of the bill to restrict this kind of disclosure only to truly life-threatening emergencies, and then only to disclose the information to those actively engaged in trying to save the life of the individual in question.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. GUDE. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. I thank the gentleman for yielding. I am not sure the amendment is necessary. I have no objection to the amendment and, as far as I know, on this side of the aisle we accept it.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. GUDE. I yield to the gentleman from Illinois.

Mr. ERLENBORN. We have had a copy of the amendment and we have no objection to it.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Maryland (Mr. Gude).

The amendment was agreed to.

AMENDMENT OFFERED BY MR. GOLDWATER

Mr. GOLDWATER. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. GOLDWATER: On page 35, after line 20, insert the following new subsection (m) to read as follows:

"(m)(1) Moratorium on the use of the social security account number—no Federal agency, or any State or local government acting in compliance with any Federal law or federally assisted program, shall deny any individual any right, benefit, or privilege provided by law by reason of such individual's refusal to disclose his social security account number.

"(2) This subsection shall not apply—

"(A) with respect to any system of records in existence and operating prior to January 1, 1975; and

"(B) when disclosure of a social security account number is required by Federal law.

"(3) No Federal agency, or any State or local government acting in compliance with any federal law or federally assisted program, shall use the social security account number for any purpose other than for verification of the identity of an individual unless such other purpose is specifically authorized by Federal law."

And, re-letter the succeeding subsecion accordingly.

Mr. GOLDWATER (during the reading). Mr. Chairman, I ask unanimous consent that the amendment be considered as read and printed in the RECORD.

The CHAIRMAN. Is there objection to the request of the gentleman from California?

There was no objection.

Mr. GOLDWATER. Mr. Chairman, I offer this amendment dealing with the use of the social security number in an attempt to bring it into proper perspective and to, in essence, put limitations upon its further use.

Every major report on the subject of personal privacy and the collection, maintenance, use and dissemination of personal information has expressed concern for the ever-growing use of the social security number as a universal numeric identifier. Almost without exception they sight the threat the unrestricted universal numeric identifier poses to the freedom and privacy of individuals. Private citizens resent the use of this number as an arbitrary precondition to the receipt of services, privileges, and benefits that are essential to their daily lives and activities. The average citizen finds the use of the number dehumanizing and threatening. Even the widely cited report of the Secretary of HEW—entitled "Records, Computers, and Rights of Citizens"—notes that there is no statutory authority for the ever-growing use of numbers as an identifier. They point out that the average citizen has no legal remedy for such use of the number. The report notes that the universal use of a numeric identifier permits the linking of files and the tracing of a person from cradle to grave. A soon to be published report—"Roscoe-Pound-American Trial Lawyers Foundation Report"—notes the negative psychological impact that has resulted from the unregulated use of this number.

In most cases, the use of this number has been resorted to in the name of efficiency. Little concern has been given for the human impact such a practice has. Everything distinctive, individual, or superior in terms of quality of a man's mind is not relevant. Everything centers on the quantitative, down with qualitive dimensions or values. The use of this number has removed the individual from the modern personal information transaction process. Records are exchanged without his knowledge and occasionally to his serious detriment. Errors are perpetuated and integrated with new records. And all of this is occurring because of administrative decisions which never analyze the larger implications of the use of the number. Simply put, the use of the number has not been subjected to the aggressive give and take that occurs in a legislative form.

Originally, the discussion draft of H.R. 16373 contained language prohibiting the further use of the social security account number as a universal numeric identifier. Objections centered on the following concerns:

First, outright prohibition would necessitate a total revamping of all Federal record systems at tremendous cost.

Second, outright prohibition is not consistent with all the best interests of citizens as it would cause chaos in many Federal programs.

The amendment I offer today remedies these problems. My amendment does the following things:

First, prohibits the denial of rights, benefits, or privileges provided by law if a citizen refuses to disclose his social security number, with the following exceptions:

The amendment exempts all systems in existence and operating prior to January 1, 1975, and would not apply when the Congress authorizes the use of the number.

The amendment restores to Congress the control over the use of the number.

This amendment will fill important voids in the current legislation. It sights a reasonable, basic compromise between the right of a citizen to protect his privacy and the need of the Federal Government to be a proper and effective servant.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. GOLDWATER. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I want to commend the gentleman for offering this amendment, the principle of which was certainly intended by the committee, but the gentleman's amendment removes any ambiguity.

I want to commend the gentleman for his diligent work, cooperation, and assistance to the subcommittee and the full committee. As far as we are concerned on this side, we will accept the amendment.

Mr. GOLDWATER. I thank the gentleman from Pennsylvania.

Mr. LAGOMARSINO. Mr. Chairman, will the gentleman yield?

Mr. GOLDWATER. I yield to my colleague from California.

(Mr. Lagomarsino asked and was given permission to revise and extend his remarks.)

Mr. LAGOMARSINO. Mr. Chairman, I would like to commend the gentleman for his amendment, and assure him of my support. I would also like to commend him for his work on the general subject.

Mr. Chairman, last year a Presidential Executive order was issued allowing the Department of Agriculture to inspect the individual tax returns of 3 million farmers—for the alleged purpose of compiling mailing lists and statistical information.

Although that order was eventually rescinded after widespread public indignation, it is a good example of the type of abuse we are trying to prevent with this bill. Not every Member of this House has a large agricultural constituency, but I ask the Members to consider that if the Department of Agriculture can obtain individual tax returns of 3 million farmers by the device of an Executive order, how many other agencies can get the individual tax returns of housewives, or barbers, or truckdrivers, on the same flimsy excuse of a need for mailing lists.

The law provides that tax returns are confidential, and the information they contain is not to be disclosed without permission. Given the events of the past few years, when tax returns become weapons to be turned against individual citizens or to punish political foes, I wonder how on Earth we can expect the ordinary citizen to comply with our income tax laws. Our system of taxation, in which we ask the individual to personally report his income and compute his tax due, relies heavily on the voluntary cooperation and basic honesty of the individual. In this respect, it is perhaps unique in the world.

Where else would you find an entire nation of people willing to report the most intimate details of their income and expenditures every year? If we had to resort to the European system of taxation, where an inspector comes by to check on your wealth and living situation, or if we had to make a detailed check of the basic facts of every income tax return filed in this country, we would be spending as much collecting this tax as we gain from it. Yet our entire system of taxation is based on the Government's assurance that individual tax returns will remain confidential—an assurance which we have seen is not always truthful.

We all remember the story of the golden goose. Well, gentlemen and ladies, if we are not careful, we are going to kill that golden goose. If we do not act now to insure the confidentiality of Government records, including private income tax returns, no one will ever again tell the truth to their Government. We have come dangerously close, I believe, to exhausting the reservoir of good will and basic honesty of the people toward their Government. If we are not honest with the public, the public will not be honest with us. One way we can assure the people that we will honor our commitments of confidentiality whenever we ask for necessary information, is to pass this bill.

Mr. Chairman, over 2,400 years ago, the Greek leader Pericles proclaimed one of the signs of a free society to be "mutual toleration of privacy." That right of privacy finds expression in both the English Magna Carta and the U.S. Bill of Rights. I believe it is time for us to lend substance to those guarantees with a statute such as the one before us today. This bill will not hamper the operation of Government, it will only make it work better, because the individual citizen will be more willing to cooperate if he knows that his privacy will remain protected. For the sake of good government, and for the sake of the people we serve, I urge an "aye" vote on this bill.

Mr. KOCH. Mr. Chairman, will the gentleman yield?

Mr. GOLDWATER. I yield to the gentleman from New York.

Mr. KOCH. Mr. Chairman, I want to commend the gentleman, my good friend from California. He has led the fight to prevent the establishment of a universal identifier number. To see that fight successfully concluded on the floor today must give him a great deal of pride and pleasure. I take pride and pleasure in his success and in having worked with him on this legislation.

Mr. GOLDWATER. I thank my friend for his support in this effort, and I urge adoption of the amendment.

Mr. ERLENBORN. Mr. Chairman, I rise in opposition to the amendment.

Mr. Chairman, the subcommittee, in considering the drafting of this bill, did consider taking under advisement whether we should include the prohibiting of a universal numeric identifier. Of course, the social security number is the most commonly used universal numeric identifier.

The problem is that to my knowledge—and I think to the knowledge of the subcommittee—there has been no study as to how many local governments or private agencies or, even, for that matter, Federal agencies, which use the universal numerical identifier or the social security number. We are not certain what effect this sort of amendment would have. I know, for instance, it is quite customary to use the social security number as the identifier on State driver's licenses. Just what effect this amendment would have, I do not think we really know, and I do not think we should pass it without knowledge. I think it would be a mistake to do this, before hearings have been held to get the facts on which to base action.

One part of the amendment would allow an exception for systems of records in operation prior to January 1, 1975. That means if a new system were to be adopted by a State or local government, it might be wholly incompatible with an existing system which is the subject of the exemption. I think we would be acting without sufficient knowledge if we were to adopt the amendment now.

I think we all want to be known by our names rather than by number so-and-so. Certainly the purpose of this amendment is worthy, but I am afraid we are acting now out of emotion rather than knowledge. We have not had any hearings on which to base action on this amendment; therefore, I think the proposal should be defeated. We should hold hearings on this subject in the near future.

The CHAIRMAN pro tempore. The question is on the amendment offered by the gentleman from California (Mr. GOLDWATER).

The amendment was agreed to.

Mr. COLLIER. Mr. Chairman, I move to strike the requisite number of words.

I do so only for one question, if I may.

Throughout the bill, the world "agency" is used, and I would like to know whether or not the word "agency" is interchangeable with the word "commission" throughout the bill.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. COLLIER. Yes, I yield to the gentleman.

Mr. ERLENBORN. As I understand the gentleman's question, it is whether regulatory commissions would be considered agencies?

Mr. COLLIER. As well as any duly appointed commissions that were authorized by the Congress, whether through Congress or through Executive appointment.

Mr. ERLENBORN. The definition of the word "agency" would be contained in the basic Freedom of Information Act, and this is the amendment to the Freedom of Information Act. My recollection is that the word "agency" defined in the act would include regulatory commissions.

Such things as study commissions, interim study commissions, or short-term study commissions, I do not believe they would be.

Mr. COLLIER. They would be excluded, notwithstanding the fact that they contain, in many instances, substantial confidential records of a personal nature?

Mr. ERLENBORN. This is only my recollection, without having a copy of the law before me. I think regulatory commissions would be included within the definition, something like the President's Commission on Population Growth in America, on which I served.

Mr. COLLIER. That is not included?

Mr. ERLENBORN. I do not believe that is included within the definition.

Mr. COLLIER. I thank the gentleman.

AMENDMENT OFFERED BY MR. BUTLER

Mr. BUTLER. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Butler; Page 23, after line 25, insert the following: "(9) pursuant to the order of a court of competent jurisdiction."

Mr. BUTLER. Mr. Chairman, this is an amendment to the section of the bill dealing with conditions of disclosure. It is introduced for the purpose of making it perfectly clear that a lawful order of a court of competent jurisdiction would be an appropriate condition of disclosure.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. BUTLER. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, the gentleman has discussed his amendment with us, and we find no objection to the amendment.

The CHAIRMAN pro tempore. The question is on the amendment offered by the gentleman from Virginia (Mr. Butler).

The amendment was agreed to.

AMENDMENT OFFERED BY MR. BUTLER

Mr. BUTLER. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Butler: On page 26, line 17, after the word "disclosure", strike out the period and add the following: "; and (5) nothing in this section shall allow an individual access to any information complied in reasonable anticipation of a civil action or proceeding."

Mr. BUTLER. Mr. Chairman, this amendment is directed to the section dealing with access to records. It is introduced for the purpose of

making it perfectly clear that an investigation of an accident or other procedures incident to problems of that nature will not be subject to inquiry or access under this section.

The amendment says:

Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. BUTLER. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, again the gentleman has been good enough to discuss this amendment with us, and we find no objection to it.

However, I would ask the gentleman this: What does he contemplate concerning the third amendment we discussed?

Mr. BUTLER. Mr. Chairman, I do not intend to introduce the third amendment the gentleman refers to.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I thank the gentleman.

We have no objection to the amendment.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. BUTLER. I yield to the gentleman from Illinois.

Mr. ERLENBORN. Mr. Chairman, as I understand it, the purpose of the amendment is to protect, as an example, the file of the U.S. attorney or the solicitor that is prepared in anticipation of the defense of a suit against the United States for accident or some such thing?

Mr. BUTLER. That is the subject we have in mind.

Mr. ERLENBORN. I appreciate the gentleman's concern. I think it is a real concern, and that protection ought to be afforded.

The only problem I find with that amendment is this: It would presuppose we intended the defining of "record system" to preclude that type of record. I do not think we did.

If these sorts of records are to be considered a record system under the act, then the agency would have to go through all the formal proceedings of defining the system, its routine uses, and publishing in the Federal Register.

Frankly, I do not think the attorney's files that are collected in anticipation of a lawsuit should be subject to the application of the act in any instance, much less the access provision. It is our concern in the access provision that it may then presuppose it is covered in the other provisions, and I do not think it should be.

Mr. BUTLER. Mr. Chairman, I share the gentleman's concern. When this amendment was originally drafted, it stated "access to any record" and we struck the word, "record," and inserted "information."

So we made it perfectly clear we were not elevating an investigation with the word, "record," to the status of records. We did want to make it clear there was not to be such access, because that access would be within the usual rules of civil procedure.

Mr. ERLENBORN. Mr. Chairman, if the gentleman will yield further, it is the gentleman's contention, under his interpretation of the act, that the other provisions would not apply to the attorney's files as well; is that correct?

Mr. BUTLER. The gentleman is correct.

Mr. ERLENBORN. I wonder if the gentleman would ask the gentleman from Pennsylvania (Mr. Moorhead) what his opinion is concerning that, just to clarify the record.

Mr. BUTLER. Mr. Chairman, I will yield to the gentleman from Pennsylvania for that purpose.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I agree with the limitation which has been placed on the amendment by the gentleman.

The CHAIRMAN pro tempore. The question is on the amendment offered by the gentleman from Virginia (Mr. BUTLER).

The amendment was agreed to.

AMENDMENT OFFERED BY MS. ABZUG

Ms. ABZUG. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Ms. Abzug: Page 33, line 3, strike out lines 3 and 4.

(Ms. ABZUG asked and was given permission to revise and extend her remarks.)

Ms. ABZUG. Mr. Chairman, we are dealing in this bill before us today with the right to privacy and any exemption from the safeguard provisions of this bill must be the exception rather than the rule. It should be justified only where there are overwhelming societal interests.

What are the overwhelming interests of society that this exemption protects which would justify an infringement on individual liberty?

Under other exemption provisions of this bill, we have already protected from disclosure information related to law enforcement investigative matters and national security.

I have agreed to support such specific exemptions. But the general exemption as to all records, regardless of what they contain, maintained by the CIA, goes too far. By allowing the CIA to exempt all systems of records, even those which contain no sensitive data, we are unnecessarily denying individuals the rights guaranteed by this bill and indeed rights guaranteed by the Constitution.

There is grave danger inherent in granting any such broad exemption. No agency should be given a general license to exempt any and all of its records or records systems.

Rather than base exemptions on the functions of an agency which maintains records, we should define exemptions, as we tried to in this bill, in terms of the kind of data sought to be protected from disclosure. We have done this in subsections (k) and (l) (1), and (2) of the bill.

If the records of the CIA contain sensitive material, these records will be protected from disclosure by the specific exemptions already referred to, information related to either foreign policy or national defense or related to investigatory material which is being compiled for law enforcement purposes.

We would weaken this bill if we established a precedent by allowing an agency to exempt itself entirely from requirements that would protect and reinforce the fundamental constitutional rights of privacy.

By setting up a general exemption guaranteeing and allowing the CIA to exempt even sensitive records from virtually every provision of the bill, the bill goes far beyond what is necessary to protect such records from disclosure. Why should not the agency be required, for

example, to keep records which are accurate, timely, and relevant, which are requirements of this bill?

Why should the agency be exempted from a bar against maintaining political or religious data if other agencies are not, and why should individuals be denied rights to civil remedies and court review?

This is the effect of the "general exemption" section of the bill, which goes far beyond the "specific exemption" section in allowing agencies to disregard the safeguard provisions of the bill.

I might tell the Members that the other body's bill does not contain any such general exemption section. It provides solely for specific exemptions, with only two of the specific ones we have, by the way, and that is for national security and law enforcement purposes.

I urge that we strike this general exemption for the CIA since the CIA's sensitive records and activities are amply protected by other provisions of this bill.

To do otherwise would be to deny unnecessarily to one group of individuals the privacy rights protected by this bill.

Mr. Chairman, I urge that my amendment be adopted.

Mr. GUDE. Mr. Chairman, will the gentlewoman yield?

Ms. ABZUG. Yes, I yield to the gentleman from Maryland.

Mr. GUDE. I want to commend the gentlewoman for this amendment.

Certainly, there is no logic in gathering information, and regardless of its sensitivity, putting it off bounds merely because it happens to be stored within a particular agency.

The gentlewoman's amendment makes a great deal of sense, and I certainly urge its adoption.

Mr. KOCH. Mr. Chairman, will the gentlewoman yield?

Ms. ABZUG. I yield to the gentleman from New York.

Mr. KOCH. I also want to commend the gentlewoman from New York, who has pointed out this particular deficiency of this legislation, which I hope will be corrected.

Mr. ERLENBORN. Mr. Chairman, I rise in opposition to the amendment.

Mr. Chairman, there are many reasons why I would oppose this amendment.

I think it is quite obvious that the activities of the Central Intelligence Agency are not the sort of activities that are supposed to be conducted in a fishbowl.

Let me make this one observation. Under this bill we are allowing any individual access to records that are maintained by the Government relative to himself. In other words, any person, any individual can go to the agency that is subject to this act and say, "I want copies of anything that you have relating to me."

In the committee we discussed whether we would extend this right to corporations. We decided we would not; we would grant it only to individuals.

We did not limit this access to U.S. citizens.

Just stop and think about this for a moment. The Central Intelligence Agency prepares and maintains files relative to people all over this country who are our potential or actual enemies.

We are not limiting access, under this law, to citizens so that Chou En-lai or whoever it might be could come over here and knock at the

door of the CIA and say, "Under the new privacy bill, I want to see all the files that you have maintained concerning me."

I think this situation would be utterly ridiculous. The amendment ought to fall of its own weight.

Ms. ABZUG. Mr. Chairman, will the gentleman yield?

Mr. ERLENBORN. I yield to the gentlewoman from New York.

Ms. ABZUG. Mr. Chairman, I just want to refresh the recollection of the gentleman from Illinois about who is covered under this bill. We have a very specific definition of individuals who are granted rights under this bill and I will quote from subsection (a)(2)—Such an individual "means a citizen of the United States or an alien lawfully admitted for permanent residence." As far as I know Chou En-lai is not a citizen of the United States or an alien lawfully admitted for permanent residence. This is just another big, big red herring.

Mr. ERLENBORN. Then maybe it would be the Ambassador of Russia; who is to say? The fact is, we ought not limit the United States to carrying on the activities of the Central Intelligence Agency in such a way that its files are kept under cellophane.

Mr. HOLIFIELD. Mr. Chairman, I move to strike the last word, and I rise in opposition to the amendment.

Mr. Chairman, I realize that there are people in this country who have a great antagonism to the CIA. I might say that back in 1947 this committee handled the legislation that established the CIA in the Defense Department bill.

We are in a dangerous world, and other countries of the world are using all the methods that they can develop for the collection of information which happens to be favorable to their objectives. Many times those objectives do not coincide with the objectives of this country, so that we, likewise, in order to protect ourselves, are collecting information on these people overseas, or the emissaries who come into this country if it deals with the national security of the United States. I believe that the better part of valor right now is to leave this alone.

Ms. ABZUG. Mr. Chairman, will the gentleman yield?

Mr. HOLIFIELD. I yield to the gentlewoman from New York.

Ms. ABZUG. Mr. Chairman, I would just like to refresh the recollection of the gentleman from California, and since he is my honorable chairman I hesitate to do this, but, nevertheless, I have pointed out that the bill provides in section (k)(1)(2) for an exemption of anything which would in any way affect the national defense or foreign policy of this Nation, so that any of the national security or foreign policy records about which the gentleman from California has expressed some concern would be amply covered. No information which in any way affects the national security or foreign policy of this Nation could, under the specific provisions of section (k) of this act, be made available.

My objection to this general blanket exemption for the CIA is that there is much information, and I am sure the gentleman from California would agree with this, that the CIA collects about individuals that is totally unrelated to the national security functions of the CIA.

Mr. HOLIFIELD. I do not know that. I am not in possession of that knowledge.

Ms. ABZUG. Even if that were not so, if an individual seeks access to his or her records and the CIA makes a determination or the agency makes a determination that access to those records would endanger our national security, then the agency would have the right to assert that reason for not providing access to the information.

All I am suggesting is that to single out one agency and exempt all its records, just because it is this agency, is quite contrary to what our purposes are, and to what our intentions are in this bill. I might also mention that the legislation in the other body has only the specific exemptions that I mentioned before. A blanket exemption for any agency—even or especially this one agency has no place in this bill.

Mr. HOLIFIELD. Mr. Chairman, let me add that this agency is charged with the security of the United States in relation to its foreign policy, and therefore important to the United States. The agency does collect information on people who are emissaries from those nations that are here, and are acting in behalf of other nations, and I just do not believe that anyone has the right or should have the right to go in and expose the most sensitive area in the protection of our national security. Therefore I must oppose the amendment.

I think we are going pretty far in this bill, and I think this is just a little bit too far.

Mr. DELLUMS. Mr. Chairman, I would like to make a point of order, and I do so because I think this matter is of such importance and such gravity that it should not be disposed of by a handful of Members, and I note that there is not a quorum present on the floor.

Therefore, Mr. Chairman, I make the point of order that a quorum is not present.

The CHAIRMAN. Evidently a quorum is not present. The Chair announces that he will vacate proceedings under the call when a quorum of the committee appears.

Members will record their presence by electronic device.

The call was taken by electronic device.

QUORUM CALL VACATED

The CHAIRMAN pro tempore (Mr. MCFALL). One hundred and four Members have appeared. A quorum of the Committee of the Whole is present. Pursuant to rule XXIII, clause 2, further proceedings under the call shall be considered as vacated.

The Committee will resume its business.

The Chair recognizes the gentleman from Pennsylvania (Mr. Moorhead).

(Mr. Moorhead of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I rise in opposition to the amendment offered by the gentlewoman from New York (Ms. Abzug). I do so with considerable regret, because of the great contribution that the gentlewoman has made in the drafting of this legislation. The gentlewoman was one of the authors of the original privacy legislation we considered. But I think in this legislation we must take a step at a time in a delicate field like that involving the Central Intelligency Agency.

Let me explain to the Members that the CIA is not entirely exempt under this bill. The agencies listed under general exemptions are affirmatively subject to the major disclosure and the requirement section of the act. The CIA must follow the conditions of disclosure, or I should say nondisclosure, as enumerated in subsection (b) of the bill. This is a major provision of the bill with which the Agency must be in compliance—with what the Agency may or may not do with their records.

The CIA is also subject to subsection (e)(2), (A) through (F) to publish in the Federal Register at least annually a notice of the existence and character of each system of records. Thus, even under the general exemption sections, they must do this.

This covers two unique circumstances: First, the Central Intelligence Agency maintains various intelligence systems, as defined by the act. Those systems maintained by the CIA are primarily personnel records. By statute the Central Intelligence Agency is prohibited from releasing any detailed information on its personnel.

The committee does not feel it should repeal other statutes by implication. Let me say also that there was an earlier colloquy between the gentlewoman from New York and the gentleman from Illinois about who is covered by the act.

On page 21, line 14, in the definitions:

> The term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence . . .

So, Mr. Chairman, I urge the defeat of the amendment.

Ms. ABZUG. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentlewoman from New York.

Ms. ABZUG. Mr. Chairman, I am very disappointed that the gentleman from Pennsylvania has to rise in opposition to my amendment. I disagree with him. I think this exemption is really out of line with the original purpose of the bill.

I had no recollection, by the way, Mr. Chairman, that the CIA ever requested this exemption, certainly not since the bill was clarified to apply only to citizens and permanent residents.

Although the gentleman has indicated what provisions the CIA, as an agency, might be subjected to, he has neglected to mention the more significant and meaningful provisions it will not be subjected to as a result of having its general exemption. I have already mentioned some of those basic provisions, such as the requirement of agencies to maintain accurate, relevant, and timely data, and I will not respect them all here.

There are many others such as this, so I do not think it is fair, even though the gentleman may oppose my amendment, for him, to suggest that a general exemption doesn't deprive individuals of basic rights provided by the act. In fact, one very seriously deprived group of individuals will be those on whom the CIA may be keeping records which have nothing at all to do with the security of this Nation.

Mr. ECKHARDT. Mr. Chairman, I rise in favor of the amendment.

Mr. Chairman, I should like to clarify that other provisions of this bill fully take care of questions having to do with security. The bill provides two types of exemptions: First, the general exemption of

agencies. In fact, only one agency is generally exempted, the Central Intelligence Agency. This is in subsection (j), "General Exemptions."

But in (k), "Specific Exemptions," it is provided on page 34, item (1) that the records within the agency are exempted from this section if the system of records is, (1) subject to the provisions of section 552(b)(1) of this title."

Now, 552(b)(1) of this title is found in the present act, and what that says is:

> This section does not apply to matters that are, (1) specifically required by Executive order to be kept secret in the interests of the national defense or foreign policy.

Executive Order 652, issued on March 8, 1972, and effective on June 1, 1972, and effective on June 1, 1972, exempts 37 agencies with respect to all matters having to do with national defenses or foreign policy. It includes, of course, the CIA. It includes the Atomic Energy Commission. It includes the State Department; it includes the Department of Defense; it includes the Justice Department.

I cannot see, for the life of me, why the CIA should be generally exempt from all provisions having to do with access if these other agencies, just as sensitive, are not also generally exempt. They deal with just as sensitive material in the area of national security as the CIA does. The point is, though, if we generally exempt the CIA from access, then the CIA does not have to come out and say that if they revealed the information, that they refuse access to, it would affect national defense or foreign policy, that it has to do with the security of the United States.

I happen to know of a case in which an employee of the CIA has been shabbily treated. I think the particular case did not have to do with security. It had to do with a girl. Some boss did not much like an inferior officer seeing her. But I shall not assert that as a fact here but as a hypothetical illustrating the evil of giving the CIA complete exemption from access provisions of this Act. The CIA can come in and say at any time, "This affects foreign affairs." But let us, at least, make them say that, because many people working for the CIA are subject to exactly the same discriminations as those working for other agencies. The CIA is going to be believed when they raise the contention that foreign affairs are affected, but at least let us make them come in and say it. Presumably, there would be some reluctance to lie about it. But if all they have to say is, "We are blanketly exempt from any access to the information which you seek," we are absolutely protecting them in matters in which the grossest discrimination could occur.

Let me just say once again that I am not talking in favor of opening up access to CIA's files with respect to matters of security, because the second exemption, the specific exemption provisions provided for in this act, refers to 552(b)(1). That says that nothing may be obtained which the Executive order requires to be kept secret in the interest of national defense or foreign policy and an Executive Order 652 has been issued and totally, blanketly covers all such matters pertaining to national defense and foreign policy.

The CHAIRMAN pro tempore (Mr. McFall). The question is on the amendment offered by the gentlewoman from New York (Ms. Abzug).

The amendment was rejected.

AMENDMENT OFFERED BY MR. ICHORD

Mr. ICHORD. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Ichord: On page 34, strike lines 7 through 11 and insert the following in lieu thereof:

"(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however*, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence."

(Mr. Ichord asked and was given permission to revise and extend his remarks.)

Mr. ICHORD. Mr. Chairman, again I wish to commend the gentleman from Pennsylvania (Mr. Moorhead) and the gentleman from Illinois (Mr. Erlenborn), as well as the members of the committee and the staff, for the very superb job they have done in balancing the rights of the individual against the rights of society in general and protecting the privacy of the individual.

All this amendment does is to protect the investigatory material of investigating agencies such as the FBI from being raided by thousands and perhaps tens of thousands of persons for no legitimate purpose.

I explained the amendment in general debate, and, Mr. Chairman, the language of this amendment has been worked out in conjunction with the managers of the bill, the gentleman from Pennsylvania (Mr. Moorhead) and the gentleman from Illinois (Mr. Erlenborn).

The purpose of this amendment is to protect our investigative agencies from activities which I do not believe is an exaggeration to say might seriously impair if not destroy their function in carrying out their vital work. The amendment would both protect this work and, at the same time, do so consistently with the attainment of the purposes and objectives of the bill. The provisions of the bill, particularly subsection (b), provides complete and adequate protection against improper or injurious dissemination of information beyond the legitimate uses of the Federal agencies maintaining them. My amendment in no way affects this laudable purpose, or those provisions against disclosure which fully protect the individual affected by prohibiting any improper use of investigatory material.

All that the amendment does is to protect the investigatory material from being raided by thousands and perhaps tens of thousands of persons for no legitimate purpose. I assure the Members that the investigative materials would be raided by the host of persons, including subversives, who would merely seek to ascertain the extent of coverage and method and adequacy of operation of our intelligence forces. This improper raiding of the investigatory files will be prohibited by my amendment, but at the same time individuals who have the legitimate need and purpose for the disclosure to them of the information is preserved. The amendment provides that in any case where an individual is denied any right, privilege, or benefit that he

would otherwise be entitled by Federal law, as a result of the maintenance of such material, he will be entitled to the information, to the extent, of course, that the identity of confidential sources will be protected.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, will the gentleman yield?

Mr. ICHORD. I yield to the gentleman from Pennsylvania.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I understand that this amendment is also subject to the colloquy we had in general debate concerning protection of dissenters under the first amendment; is that correct?

Mr. ICHORD. The gentleman is correct. This is meant in no way to harm the first amendment rights of any American.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, with that understanding, I have no objection to the amendment.

The CHAIRMAN pro tempore (Mr. McFall). The question is on the amendment offered by the gentleman from Missouri (Mr. Ichord).

The amendment was agreed to.

AMENDMENT OFFERED BY MR. GUDE

Mr. GUDE. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. GUDE: Page 36, line 6, after the period, insert the following:

"(n) Federal Privacy Commission

"(i) Establishment of Commission—

"(A) There is established as an independent agency of the executive branch of the government the Federal Privacy Commission.

"(B)(i) The Commission shall be composed of five members who shall be appointed by the President, by and with the advice and consent of the Senate, from among members of the public at large who, by reason of their knowledge and expertise in any of the following areas: civil rights and liberties, law, social sciences, and computer technology, business, and State and local government, are well qualified for service on the Commission and who are not otherwise officers or employees of the United States. Not more than three of the members of the Commission shall be adherents of the same political party.

"(ii) One of the Commissioners shall be appointed Chairman by the President.

"(iii) A Commissioner appointed as Chairman shall serve as Chairman until the expiration of his term as a Commissioner of the Commission (except that he may continue to serve as Chairman for so long as he remains a Commissioner and his successor as Chairman has not taken office). An individual may be appointed as a Commissioner at the same time he is appointed Chairman.

"(C) The Chairman shall preside at all meetings of the Commission and a quorum for the transaction of business shall consist of at least three members present (but the Chairman may designate an Acting Chairman who may preside in the absence of the Chairman). Each member of the Commission, including the Chairman shall have equal responsibility and authority in all decisions and actions of the Commission, shall have full access to all information relating to the performance of his duties or responsibilities, and shall have one vote. Action of the Commission shall be determined by a majority vote of the members present. The Chairman (or Acting Chairman) shall be the official spokesman of the Commission in its relations with the Congress. Government agencies, persons, or the public, and, on behalf of the Commission, shall see to the faithful execution of the policies and decisions of the Commission, and shall report thereon to the Commission from time to time or as the Commission may direct.

"(D) Each Commissioner shall be compensated at the rate provided for under section 5314 of title 5 of the United States Code, relating to level IV of the Executive Schedule.

"(E) Commissioners shall serve for terms of three years. No Commissioner may serve more than two terms. Vacancies in the membership of the Commission shall be filled in the same manner in which the original appointment was made.

"(F) Vacancies in the membership of the Commission, as long as there are three Commissioners in office, shall not impair the power of the Commission to execute the functions and powers of the Commission.

"(G) The members of the Commission shall not engage in any other employment during their tenure as members of the Commission.

"(2) Personnel of the Commission—

"(A) The Commission shall appoint an Executive Director who shall perform such duties as the Commission may determine. Such appointment may be made without regard to the provisions of title 5, United States Code.

"(B) The Executive Director shall be compensated at a rate not in excess of the maximum rate for GS–18 of the General Schedule under section 5332 of title 5, United States Code.

"(C) The Commission is authorized to appoint and fix the compensation of such officers and employees, and prescribe their functions and duties, as may be necessary to carry out the provisions of this section.

"(D) The Commission may obtain the services of experts and consultants in accordance with the provisions of section 3109 of title 5, United States Code.

"(3) Functions of the Commission. The Commission shall—

"(A) publish annually a United States Directory of Information Systems containing the information specified to provide notice under subsection (e)(2) of this section for each information system subject to the provisions of this section and a listing of all statutes which require the collection of such information by a Federal agency;

"(B) investigate, determine, and report any violation of any provision of this section (or any regulation adopted pursuant thereto) to the President, the Attorney General, the Congress, and the General Services Administration where the duties of that agency are involved, and to the Comptroller General when it deems appropriate; and

"(C) develop model guidelines for the implementation of this section and assist Federal agencies in preparing regulations and meeting technical and administrative requirements of this section.

"(D) In additional to its other functions the Commission shall—

"(i) to the fullest extent practicable, consult with the heads of appropriate departments, agencies, and instrumentalities of the Federal Government in carrying out the provisions of this section;

"(ii) perform or cause to be performed such research activities as may be necessary to implement the provisions of this section and to assist Federal agencies in complying with the requirements of this section;

"(iii) determine what specific categories of information should be prohibited by statute from collection by Federal agencies on the basis that the collection of such information would violate an individual's right of privacy.

"(4) Confidentiality of Information—

"(A) Each department, agency, and instrumentality of the executive branch of the Government, including each independent agency, shall furnish to the Commission, upon request made by the Chairman, such data, reports, and other information as the Commission deems necessary to carry out its functions under this section.

"(B) In carrying out its functions and exercising its powers under this section, the Commission may accept from any Federal agency or other person any identifiable personal data if such data is necessary to carry out such powers and functions. In any case in which the Commission accepts any such information, it shall provide appropriate safeguards to insure that the confidentiality of such information is maintained and that upon completion of the purpose for which such information is required it is destroyed or returned to the agency or person from which it is obtained, as appropriate.

"(5) Powers of the Commission—

"(A) The Commission may, in carrying out its functions under this section, conduct such inspections, sit and act at such times and places, hold such hearings, take such testimony, require by subpena the attendance of such witnesses and the production of such books, records, papers, correspondence, and documents, ad-

minister such oaths, have such printing and binding done, and make such expenditures as the Commission deems advisable. Subpenas shall be issued under the signature of the Chairman or any member of the Commission designated by the Chairman and shall be served by any person designated by the Chairman or any such member. Any member of the Commission may administer oaths or affirmations to witnesses appearing before the Commission.

"(i) In case of disobedience to a subpena issued under subparagraph (A) of this subsection, the Commission may invoke the aid of any district court of the United States in requiring compliance with such subpena. Any district court of the United States within the jurisdiction where such person is found or transacts business may, in case of contumacy or refusal to obey a subpena issued by the Commission, issue an order requiring such person to appear and testify, to produce such books, records, papers, correspondence, and documents, and any failure to obey the order of the court shall be punished by the court as a contempt thereof.

"(ii) Appearances by the Commission under this section shall be in its own name. The Commission shall be represented by attorneys designated by it.

"(B) Section 6001(1) of title 18, United States Code, is amended by inserting immediately after "Securities and Exchange Commission," the following: "the Federal Privacy Commission."

"(C) The Commission may delegate any of its functions to such officers and employees of the Commission as the Commission may designate and may authorize such successive redelegations of such functions as it may deem desirable.

"(D) In order to carry out the provisions of this section, the Commission is authorized—

"(i) to adopt, amend, and repeal rules and regulations governing the manner of its operations, organization, and personnel;

"(ii) to adopt, amend, and repeal interpretative rules for the implementation of the rights, standards, and safeguards provided under this section;

"(iii) to enter into contracts or other arrangements or modifications thereof, with any government, any agency or department of the United States, or with any person, firm, association, or corporation, and such contracts or other arrangements, or modifications thereof, may be entered into without legal consideration, without performance or other bonds, and without regard to section 3709 of the Revised Statutes, as amended (51 U.S.C. 5);

"(iv) to make advance, progress, and other payments which the Commission deems necessary under this section without regard to the provisions of section 3648 of the Revised Statutes, as amended (31 U.S.C. 529);

"(v) receive complaints of violations of this Act and regulations adopted pursuant thereto; and

"(vi) to take such other action as may be necessary to carry out the provisions of this section.

"(6) Reports—

"The Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this section."

Mr. GUDE (during the reading). Mr. Chairman, I ask unanimous consent that the amendment be considered as read and printed in the RECORD.

The CHAIRMAN pro tempore. Is there objection to the request of the gentleman from Maryland?

There was no objection.

Mr. GUDE. Mr. Chairman, this amendment establishes a Federal Privacy Commission which is a vital necessity if privacy legislation is to become a meaningful statute. Clearly the key to the maintenance of successful privacy standards will be the degree of cooperation provided by federal agencies which have to implement the program. This Commission, which would coordinate and assist in those efforts, will be an important tool for gaining the necessary agency cooperation.

The Commission would be composed of five full time members appointed by the President with the advice and consent of the Senate. The functions of the Commission would be to:

First, publish annually a Directory of Information System containing data on Federal agency information systems and the statutes which require the collection of information;

Second, investigate and report agency violations of this section of the bill;

Third, develop model guidelines and provide assistance to federal agencies for the implementation of this section;

Fourth, provide consultation and research services to aid agencies in carrying out the provisions of this section; and

Fifth, determine what categories of information Federal agencies should be forbidden to collect.

To fulfill these responsibilities the Commission would have rulemaking authority, the power to hold hearings, administer oaths and receive evidence, including complaints of violations of provisions of the Act, and subpena power. Additionally the Commission could gain access to any agency information system and any identifiable information, so long as appropriate safeguards are maintained to insure confidentiality.

The Commission's powers are more limited than those provided in other earlier proposals. For example, its activities are limited to concern with the provisions of this act and not any other freedom of information legislation; and it will not be able to issue orders directing an agency to comply with the requirements of the act. However, the Commission will serve as a focus of attention for information and privacy issues and will also be a watchdog over agencies which are responsible for implementing the provisions of the act.

In my view, this Commission would be an essential element in the implementation of privacy legislation. As the bill presently reads, it contains no provision for the establishment of an administrative body to oversee implementation of the legislation. I know some say we should take a "wait and see" attitude about a privacy commission.

However, such a "wait and see" attitude is exactly the opposite of what is needed, because the major problems of implementation and the inevitable adjustments in the ways agencies work are going to occur at the beginning of the program, not later on. At a minimum, this Commission should be established to oversee, monitor, and evaluate the newly legislated safeguard requirements and to offer information and assistance to Federal agencies in their efforts to comply with the act. As with any new program, there will be problems and these problems will occur in the beginning when the program is being set up. A central source of expertise and guidance and a coordinated approach to these problems should serve to reduce rather than increase administrative costs over the long run.

Moreover, we would be more than naive if we failed to recognize that individual Federal agencies cannot be expected to take an aggressive role in enforcing privacy legislation. Enforcement of the provisions of this bill will be secondary to each agency's legislative mandate and will, of necessity, cause some inconvenience. I believe it is clear that making administration of privacy standards every agency's responsibility really means making it no agency's responsibility. Only by providing a separate independent agency to act as a focus for privacy activities and concerns and for coordinating the privacy pro-

grams of the various Federal agencies can we be assured of uniform effective enforcement of the rights guaranteed by this bill.

Mr. Chairman, this Commission is very much in the interest of getting legislation which affects the privacy of all American citizens and specifically Federal employees. I very much hope and urge that the committee will adopt this amendment.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I rise in opposition to the amendment.

(Mr. Moorhead of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I rise in opposition to this amendment with great regret, because the gentleman from Maryland was one of the most productive members of the subcommittee in helping draft this legislation.

I do have to oppose the amendment, first, because it was considered in subcommittee and voted down. Second, it was considered in the full committee, and it was voted down.

I can understand why the gentleman from Maryland asked unanimous consent to dispense with the reading of the amendment, because it is a long, three-page amendment. It is really a bill in and of itself.

I do oppose this amendment to create a Federal privacy commission for a number of important reasons.

First, as I say, it was voted down at the markup session. It was overwhelmingly defeated.

Second, it would add to the overall cost of the bill and create another level of bureaucracy between the citizen and the Federal agency and his right to his own personal records.

Third, it could impede the operation of the various civil remedies afforded to individual Americans in the courts.

Fourth, as President Ford stated in his remarks referred to earlier in the debate:

> I do not favor establishing a separate commission or board bureaucracy empowered to define privacy in its own terms and to second-guess citizens and agencies.

It seems to me that it would be better to have an independent branch of the Government, that is, the judicial branch, oversee the Executive rather than another branch of the executive overseeing the Executive.

Finally, if, in this instance, the courts do not do the excellent job they have done under the Freedom of Information Act, then we in Congress can always in the future create a privacy board.

But if we create this commission it will surely develop its own constituency, and be extremely difficult to reverse if we have made a mistake.

Instead, Mr. Chairman, this bill, patterned after the Freedom of Information Act, makes each agency directly responsible, and publicly and legally accountable for its faithful administration of this law. I am sure that the courts will do their duty. Vigorous congressional oversight will also help keep the bureaucracy in line.

I can assure the Members that our committee will fully exercise such authority. Therefore, I urge the defeat of the amendment.

Mr. HOLIFIELD. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from California.

Mr. HOLIFIELD. Mr. Chairman, I am pleased with the statement made by the gentleman from Pennsylvania. As the gentleman has stated, this creates another bureau to watch the watchers, one might say, and it also gives this commission some powers to make recommendations, rules, and regulations on the basis of their judgment rather than upon the basis of the language of the bill, which I think is adequate enough to give the citizens a right.

It also would mean that undoubtedly people who were dissatisfied would go to the commission for relief, rather than to let their wishes be known to the courts, or if they did not want to go to the courts to go to the committee, which will have continuing oversight over this.

This is a committee which has had the interest to hold the hearings, and develop this bill after a great many consultations with people in the Department of Justice and other departments of the Government, and also with representatives of the administration. The President even went out of his way in his message on October 9 to say specifically that we should not create a commission, as the gentleman from Pennsylvania has mentioned.

So, for that reason, as well as others, I think this ought to be voted down. In making that statement, may I add further that I certainly do not want to disparage the attitude or the industry of the gentleman from Maryland (Mr. Gude), who has been a fine member of our committee.

Mr. ERLENBORN. Mr. Chairman, I move to strike the requisite number of words, and I rise in opposition to the amendment.

(Mr. Erlenborn, asked and was given permission to revise and extend his remarks.)

Mr. ERLENBORN. Mr. Chairman, I join the gentleman from Pennsylvania (Mr. MOORHEAD) in opposing the amendment. I think the gentleman from Pennsylvania has very well articulated the reasons the amendment should be opposed. Therefore, I hope the amendment will be defeated.

Ms. ABZUG. Mr. Chairman, I move to strike the requisite number of words, and I rise in favor of the amendment.

(Ms. Abzug asked and was given permission to revise and extend her remarks.)

Ms. ABZUG. Mr. Chairman, I really am somewhat surprised to hear the gentlemen oppose this Commission, since this commission was modeled on a bill, H.R. 4960, which was introduced in February 1973, by Mr. Horton, and cosponsored by Mr. Erlenborn, and of course Mr. Gude, who is the author of the amendment, Mr. Hanrahan, Mr. McCloskey, Mr. Moorhead, my distinguished chairman, Mr. Pritchard, Mr. Regula, and Mr. Thone. It is basically the same Commission that was proposed in the legislation originated by these gentleman, and I am finding it very difficult to figure out why they have changed their minds.

Mr. ERLENBORN. Mr. Chairman, will the gentlewoman yield?

Ms. ABZUG. Well, I guess so.

Mr. ERLENBORN. Mr. Chairman, I thank the gentlewoman for her gracious yielding to me.

The bill that the gentlewoman has referred to, of course, was not a privacy commission because we did not have a privacy bill before us

at the time, or a privacy act; that was a Freedom of Information Commission.

Ms. ABZUG. I understand it was a Freedom of Information Commission, and the fact is that the same reasons that it was proposed there are the same reasons it was proposed here. I believe we should have a commission which covers both the Freedom of Information Act and this Privacy Act. But this Commission is being proposed by the gentleman from Maryland (Mr. Gude) only for the privacy act, and there is good reason for this.

For example, the bill which is before the other body, which is the counterpart of our bill, provides for a privacy commission. We are charting an important course and, quite contrary to what my colleagues have suggested, we have not proposed any judicial or quasi-judicial functions for this Commission.

We are not proposing a superagency with enforcement powers over other agencies. Quite to the contrary, what we are doing is suggesting that there be a mechanism established which will help us in the implementation of this very important Privacy Act. One of the specific needs will be to insure that in developing rules and guidelines relating to personal information systems, agencies will have the benefit of some expertise and will achieve some degree of uniformity.

So it will really make it easier and more economical to implement this legislation.

I find it very interesting that it was suggested that we had a full hearing on this matter before our full committee. If I may refresh the recollection of my subcommittee chairman, it is true that we raised it in the subcommittee. It is true it was defeated in the subcommittee. As a matter of fact, when I pointed out that this was patterned after the bill of the members of the committee, they thought they would like to reconsider it. But this amendment was never considered in full committee, because I was interested in helping the bill get to the floor, and I said we would bring these amendments up on the floor instead.

I am a little surprised, if I may have the attention of the Chairman. I was contradicting him, and I thought he should hear me contradict him. It would be impolite of me not to call it to his attention. We certainly did not have action on this in the full committee, but only in the subcommittee. In the full committee, if the Chairman will recall, I yielded to the desire of everyone to bring a bill to the floor, and we said we would bring up amendments on the floor.

As a matter of fact, I had the impression that this amendment would be favorably supported by the ranking members of the committee, as well as the Chairman, when the gentleman from Maryland (Mr. Gude) proposed it.

If we want to make this bill significantly workable and effective, it needs just such a commission. Without it, there will be confusion; there will be chaos. Each agency will act like a lord making different regulations come about in different ways. This amendment would furnish a mechanism which could really help this act to become effective.

I heartily support this amendment.

Mr. GUDE. Mr. Chairman, will the gentlewoman yield?

Ms. ABZUG. I yield to the gentleman from Maryland.

Mr. GUDE. I thank the gentlewoman for yielding.

I want to thank the gentlewoman for her remarks. Certainly there is no Member of Congress who is not aware of the variation of the agencies of the Federal Government as far as their interest in the sensitivity of citizens' rights. We can see some agencies going off in one direction, unconcerned about privacy, and others complying with this bill. We need this commission desperately.

Mr. KOCH. Mr. Chairman, I move to strike the requisite number of words, and I rise in support of the amendment offered by the gentleman from Maryland (Mr. Gude).

The Federal Privacy Board was incorporated into the original legislation which I first initiated, and I have always supported that Board. I recognize that reasonable people can disagree on any matter, and I recognize the disagreement here. Arguments have been given on both sides, and while I support the Federal Privacy Board, I do not for a moment believe that those who are in opposition do so because they want to weaken the legislation. It is a philosophical matter as to whether or not we want to introduce what some have called another layer of Government.

What I should like to point out to the Members is that whether we call it a Federal Privacy Board and give it independent status, or pass the legislation without the Federal Privacy Board in accordance with the Gude amendment, we must have some kind of a privacy board to regulate what will happen, and the functions of the Federal Privacy Board will be executed probably by OMB. But they will not be able to execute them as well, as efficiently, as ably as a Federal Privacy Board given the powers that the Gude amendment would give to it. I think it is a very important amendment. I am pleased that the Senate has that provision in its bill.

I would hope that ultimately whatever legislation is enacted by both Houses of this Congress we will incorporate this in the Federal privacy bill.

The CHAIRMAN. The question is on the amendment offered by the gentleman from Maryland (Mr. Gude).

The question was taken; and on a division (demanded by Mr. Gude) there were—ayes 9, noes 29.

So the amendment was rejected.

AMENDMENT OFFERED BY MR. KOCH

Mr. KOCH. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Mr. Koch: Page 29, line 24, immediately after "subsection" insert "and agency notices published under subsection (e)(2) of this section".

Mr. KOCH. Mr. Chairman, I discussed this amendment with both sides of the aisle and if I understand it correctly it is acceptable to them, so I will not belabor the point. It merely requires that the Office of the Federal Register shall annually compile and publish rules and notices as opposed to rules as now provided in the bill itself.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, if the gentleman will yield, we have no objection to the amendment.

Mr. ERLENBORN. Mr. Chairman, if the gentleman will yield, we have no objection.

Mr. GOLDWATER. Mr. Chairman, will the gentleman yield?

Mr. KOCH. I yield to the gentleman from California.

(Mr. Goldwater asked and was given permission to revise and extend his remarks.)

Mr. GOLDWATER. Mr. Chairman, I rise in support of the amendment presented by my colleague from New York (Mr. Koch). A directory describing each personal information system is a vital tool for the citizen. Without it, he could search fruitlessly for particular data banks among the more than 850 in the Federal Government to do more than end secrecy about the existence of personal information they keep. We must pull away the cloak of mystery about how to get access to personal files or obtain a copy by mail.

The legislation before us provides only for printing the existence and character of these personal information systems in the Federal Register? This would mean up to 900 different entries could be spread over a 12-month period. Asking individuals to wade through copies of the Federal Register is foolhardy. Simply cataloging agencywide regulations will similarly frustrate the citizen searching for a specific system.

Mr. Chairman, the corrective language proposed by Mr. Koch will give us the directory of Federal data banks we need and I urge its adoption.

The CHAIRMAN. The question is on the amendment offered by the gentleman from New York (Mr. Koch).

The amendment was agreed to.

AMENDMENT OFFERED BY MS. ABZUG

Ms. ABZUG. Mr. Chairman, I offer an amendment.

The Clerk read as follows:

Amendment offered by Ms. Abzug: Page 34, line 12, strike out line 12 and all that follows through line 14.

Page 34, line 15, change "(4)" to "(3)".

(Ms. Abzug asked and was given permission to revise and extend her remarks.)

Ms. ABZUG. Mr. Chairman, I object to this exemption for many of the same reasons that I objected to the general exemption for the CIA. Exemptions should be defined in specific terms and in terms related to the societal interest or public policy to be served.

Yet, here again, we have defined the exemption in terms of the function of the agency rather than in terms of the nature of the records. What sensitive data are we seeking to protect by allowing the Secret Service to exempt all its records from the requirements of the bill?

The committee report tells us on page 19 that:

Access to Secret Service intelligence files on certain individuals would vitiate a critical part of Secret Service work which was specifically recommended by the Warren Commission....

This is ridiculous. I read the Warren Commission report. What did it recommend? What it recommended was that there be maintenance of more selective files in a more efficient and sophisticated manner, specifically, for example, by conversion to automatic data processing.

I am not convinced that the maintenance of some 84,000 files—which

is the number of files maintained by the Secret Service, according to the Ervin Subcommittee on Constitution Rights report just issued—is any indication that the Secret Service is now doing a better job of "attempting to identify those persons who might prove a danger to the President." The mere size of this group may indicate quite the contrary; but that also is not the point.

Even assuming that these files must be maintained and perhaps there is justification for maintaining some 300 or 400 files I fail to see the connection between this exemption and the Warren Commission recommendations. How would access to one's files interfere with the mandate of the Secret Service?

As a matter of fact, the Ervin Subcommittee on Constitutional Rights made a comment about this and they said that withholding permission for revision of files by individuals concerned would seem to serve no valid purpose. Surely the Secret Service has nothing to gain by maintaining erroneous information that can be corrected by individuals—and that is one of the prime rights under this act. If we are trying to prevent acts of violence, how does disclosure of information defeat that goal? An argument could well be made that such disclosure would, in fact, act as a deterrent.

So before voting on this amendment, it should be clear to all of you that the striking of the proposed exemption will have absolutely no effect on the essential work of the Secret Service, which is the maintenance of accurate and selective files. It will have no effect on its functions. All I am saying is, if there are Secret Service files, as indeed there are, they have enough protection under the exemption provisions of this act. But if there are people's names listed galore, as we know there are in their files, because they said they disagreed with what somebody in Government said, they have a right to know what cranks are making statements against them. They have a right to correct their files. They have a right to know whether their privacy is being invaded.

I think it is shocking that we should take a particular agency and give it a blanket exemption, when there is ample protection under the act. We are again sacrificing basic individual rights of privacy for some strange reason that is mumbo-jumbo.

If one mentions the CIA, he cannot do a thing. If one mentions the Secret Service, he cannot do a thing. It is time we stopped this mindless mentioning of agencies and accomplish the real purpose of this bill.

I urge support of my amendment.

Mr. Erlenborn. Mr. Chairman, I rise in opposition to the amendment.

Mr. Chairman, the amendment would strike the specific exemption provision on page 34, lines 12 through 14, of the protective services of the President of the United States.

This does not exempt particularly from the operation of the bill the maintenance of these records. The sections that could be under regulations exempted are (c) (3), (d), (e) (1) (2) (G) and (H).

Now, if I am interpreting this correctly, and I think I am, this still would require an identification of the system under section (e) (1), lines 11 through 24.

That would require that in the Federal Register the following things be published:

"(A) the name and location of the system;
"(B) the categories of individuals on whom records are maintained in the system;
"(C) the categories of records maintained in the system;
"(D) each routine purpose for which the records contained in the system are used or intended to be used, including the categories of users of the records for each such purpose;
"(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
"(F) the title and business address of the agency official who is responsible for the system of records;

That means that many of the provisions of the act, and I think also including the prohibition of transfer to other agencies, except for those purposes that have been identified as routine uses, will be applicable to these records.

I think the only real harm we could envision would be transfer of this information to some other agency where the person would be harmed in his application for employment or some other right or privilege under the laws of the United States.

Since these other provisions are still applicable to the system, I think that the specific exemption here providing that access not be made available to the persons who are named in the system is a valid exemption, one that is necessary. It falls under the same general category of law enforcement where we already have an exemption. Therefore, I think the amendment should be defeated.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I rise in opposition to the amendment.

(Mr. Moorhead of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, there is much of the criticism of the Secret Service by the gentlewoman from New York that is correct. The list of the protective service by the Secret Service has gotten too broad. It does contain names of people who are not a real threat, but merely dissidents exercising the American right of dissent.

But, on the other hand, the list also contains the names of people who are a real threat, and they contain informers and information about the techniques of protection. We have to recognize that in this day and age, unfortunately, assassination, holding hostage and killing has become too prevalent so that an amendment which completely eliminates the secrecy of the legitimate protective right of the Secret Service just goes too far.

As I have discussed with the gentleman from Illinois (Mr. ERLENBORN) and as we have said to the gentlewoman from New York (Ms. ABZUG), we intend to hold a hearing and hold the feet of the Secret Service to the fire to weed out and make this list really something small so that they can be effective. If it is a broad list, it really does not do the job we want to have done to protect not only the President, but other officers of the Government and visiting dignitaries.

It seems to me that the amendment goes too far. We cannot be sure they would be exempt under other exemptions, and I think the cor-

rect way to proceed, as I have promised, is to hold intensive, hard-hitting hearings next year.

I would ask the gentleman from Illinois if, as he told me in private, he would cooperate fully in this endeavor.

Mr. ERLENBORN. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the gentleman from Illinois.

Mr. ERLENBORN. Mr. Chairman, I agree with the gentleman, and I hope we will hold those hearings early in the next Congress.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I thank the gentleman, and I urge the defeat of the amendment.

The CHAIRMAN pro tempore (Mr. Brademas). The question is on the amendment offered by the gentlewoman from New York (Ms. Abzug).

The amendment was rejected.

Mr. MOORHEAD of Pennsylvania. Mr. Chairman, I move to strike the requisite number of words.

Mr. Chairman, before the Committees rises, I wish to summarize briefly the present situation on the privacy bill. On October 9, President Ford issued a statement, which I include at this point in the Record, endorsing H.R. 16373, the Privacy Act of 1974:

STATEMENT BY THE PRESIDENT

Legislation to protect personal privacy is making significant progress in the Congress. I am delighted about the prospect of House and Senate action at this session.

Renewed national efforts to strengthen protections for personal privacy should begin in Washington. We should start by enacting uniform fair information practices for the agencies of the Federal government. This will give us an invaluable operating experience as we continue to examine and recommend needed actions at the State and local level and in the private sector.

The immediate objective should be to give every citizen the right to inspect, challenge and correct, if necessary, information about him contained in Federal agency records and to assure him a remedy for illegal invasions of privacy by Federal agencies accountable for safeguarding his records. In legislating, the right of privacy, of course, must be balanced against equally valid public interests in freedom of information, national defense, foreign policy, law enforcement, and in a high quality and trustworthy Federal work force.

Immediately after I assumed the chairmanship, as Vice President, of the Cabinet-level Domestic Council Committee on the Right of Privacy, I asked the Office of Management and Budget to work jointly with the Committee staff, the Executive agencies and the Congress to work out realistic and effective legislation at the earliest possible time. Substantial progress has been made by both the Senate and the House on bills extending personal privacy protections to tens of millions of records containing personal information in hundreds of Federal data banks.

H.R. 16373, the Privacy Act of 1974, has my enthusiastic support, except for the provisions which allow unlimited individual access to records vital to determining eligibility and promotion in the Federal service and access to classified information. I strongly urge floor amendments permitting workable exemptions to accommodate these situations.

The Senate, also, has made substantial progress in writing privacy legislation. S. 3418 parallels the House bill in many respects, but I believe major technical and substantive amendments are needed to perfect the bill. I do not favor establishing a separate Commission or Board bureaucracy empowered to define privacy in its own terms and to second guess citizens and agencies. I vastly prefer an approach which makes Federal agencies fully and publicly accountable for legally mandated privacy protections and which gives the individual adequate legal remedies to enforce what he deems to be his own best privacy interests.

The adequate protection of personal privacy requires legislative and executive initiatives in areas not addressed by H.R. 16373 and S. 3418. I have asked Executive branch officials to continue to work with the Congress to assure swift action on measures to strengthen privacy and confidentiality in income tax records, criminal justice records and other areas identified as needed privacy initiatives by the Domestic Council Committee on the Right of Privacy.

He made two points on which this endorsement was conditioned—

First, adoption of what has been embodied in the Erlenborn amendment; and

Second, defeat of any amendment calling for creation of a so-called Privacy Commission.

Mr. Chairman, both of these conditions have been met. While I personally opposed the Erlenborn amendment and voted against it, it was nevertheless adopted yesterday on a 192 to 177 recorded vote. The amendment to establish a Privacy Commission, offered by the gentleman from Maryland (Mr. Gude) earlier today, was defeated.

Mr. Chairman, this bill, as now before use, therefore meets the specific criteria set forth for privacy legislation by President Ford last month. I urge Members on both sides of the aisle to give it the same enthusiastic support as that expressed by President Ford and by many others from all parts of the political spectrum. We do not claim that will solve all of the privacy problems which abound in modern society. It is not a perfect bill: But it is a start and an important first step in the right direction.

Mr. Chairman, section 522a(b)(2) of the bill allows an agency to disclose records contained in a system of records "for a routine use described in any rule * * *."

It would be an impossible legislative task to attempt to set forth all of the appropriate uses of Federal records about an identifiable individual. It is not the purpose of the bill to restrict such ordinary uses of the information. Rather than attempting to specify each proper use of such records, the bill gives each Federal agency the authority to set forth the "routine" purposes for which the records are to be used under the guidance contained in the committee's report.

In this sense "routine use" does not encompass merely the common and ordinary uses to which records are put, but also includes all of the proper and necessary uses even if any such use occurs infrequently. For example, individual income tax return records are routinely used for auditing the determination of the amount of tax due and for assistance in collection of such tax by civil proceedings. They are less often used, however, for referral to the Justice Department for possible criminal prosecution in the event of possible fraud or tax evasion, though no one would argue that such referral is improper; thus the "routine" use of such records and subsection (b)(2) might be appropriately construed to permit the Internal Revenue Service to list in its regulations such a referral as a "routine use."

Again, if a Federal agency such as the Housing and Urban Development Department or the Small Business Administration were to discover a possible fraudulent scheme in one of its programs it could "routinely," as it does today, refer the relevant records to the Department of Justice, or its investigatory arm, the FBI.

Mr. Chairman, the bill obviously is not intended to prohibit such necessary exchanges of information, providing its rulemaking proce-

dures are followed. It is intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes. To this end it would be sufficient if an agency publishes as a "routine use" of its information gathered in any program that an apparent violation of the law will be referred to the appropriate law enforcement authorities for investigation and possible criminal prosecution, civil court action, or regulatory order.

It should be noted that the "routine use" exception is in addition to the exception provided for dissemination for law enforcement activity under subsection (b)(6) of the bill. Thus a requested record may be disseminated under either the "routine use" exception, the "law enforcement" exception, or both sections, depending on the circumstances of the case.

Mr. Chairman, section 552a(b)(6) authorizes dissemination of records contained in a system of records "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request * * *."

The words "head of the agency" deserve elaboration. The committee recognizes that the heads of Government departments cannot be expected to personally request each of the thousands of records which may properly be disseminated under this subsection. If that were required, such officials could not perform their other duties, and in many cases, they could not even perform record requesting duties alone. Such duties may be delegated, like other duties, to other officials, when absolutely necessary but never below a section chief, and this is what is contemplated by subsection (b)(6). The Attorney General, for example, will have the power to delegate the authority to request the thousands of records which may be required for the operation of the Justice Department under this section.

Mr. Chairman, "agency" is given the meaning which it carries elsewhere in the Freedom of Information Act, 5 United States Code, section 551(1), as amended by H.R. 12471 of this Congress, section 552(e), on which Congress has acted to override the veto. The present bill is intended to give "agency" its broadest statutory meaning. This will permit employees and officers of the agency which maintains the records to have access to such records if they have a need for them in the performance of their duties. For example, within the Justice Department—which is an agency under the bill—transfer between divisions of the Department, the U.S. Attorneys' offices, the Parole Board, and the Federal Bureau of Investigation, would be on a need-for-the-record basis. Transfer outside the Justice Department to other agencies would be more specifically regulated. Thus, transfer of information between the FBI and the Criminal Division of the Justice Department for official purposes would not require additional showing or authority, in contrast to transfer of such information from the FBI to the Labor Department.

Mr. Chairman, this bill is not designed to interfere with access to information by the courts. Thus a court is not defined as an "agency" nor is it intended to be a "person" for purposes of this legislation. Therefore, the necessary orderly flow of information from Government

agencies to the courts will not be impeded. The Congress is treated similarly to the courts; it is also excluded from the definition of "agency."

Mr. HOLIFIELD. Mr. Chairman, will the gentleman yield?

Mr. MOORHEAD of Pennsylvania. I yield to the distinguished chairman of the full committee, the gentleman from California (Mr. Holifield).

Mr. HOLIFIELD. Mr. Chairman, at this time I would like to pay tribute to the chairman of the subcommittee and the ranking minority member of that subcommittee, and all of the members of the subcommittee who participated in this very long and laborious and important bill. It is a complicated bill and treads new ground, as the subcommittee chairman has said. It may not be as complete as some would want, and it may have some things in it others do not want.

It is something I think that the House can get behind, and I do know the deep interest of the gentleman from Pennsylvania and the gentleman from Illinois in this subject matter, as well as the other Members of the committee, and I know that their oversight on this will be an active and living oversight in the days to come. You cannot grow a full-grown oak by one act, planting. Every piece of legislation that I have worked on in the 32 years I have been here has had to be supervised by the committee or attended to and changed from time to time, with changing conditions, or with information that comes in that indicates changes are necessary. I want to commend both of the gentlemen and members of the committee for work they have done on this. I believe it is a good bill and I intend to vote for it.

Mr. MOORHEAD of Pennsylvania. I thank the gentleman for his kind remarks.

(Mr. Moorhead of Pennsylvania asked and was given permission to revise and extend his remarks.)

Mr. KEMP. Mr. Chairman, I rise in support of the bill H.R. 16373, the proposed Privacy Act of 1974, and the principles embodied within it. The American people deserve the type of protection of their privacy provided by this legislation and I ask that it be passed overwhelmingly.

This is not a new subject area to me.

During this Congress I have sponsored or cosponsored 16 separate measures relating to the right of privacy. These measures would tighten policy and procedures in such practices as the exchange of information about individuals between Government agencies and Government and industry; the use of social security numbers and other coding systems as universal identifiers; the procedures for approval of wiretaps and other forms of electronic surveillance; the inspection of confidential Federal income tax returns by unauthorized parties; the scope of the exclusions from the Freedom of Information Act; and various forms of surveillance.

As a member of the Task Force on Privacy, the extensive final report of which was released several months ago, I had an opportunity to participate in the formulation of specific recommendations on what actions the Congress ought to take to further assure the adequacy of law as to the right of privacy.

And, as a member of the Committee on Education and Labor, I was deeply involved in—and supportive of—the enactment of the recent

amendment to the Elementary and Secondary Education Act, an amendment tightening procedures for disclosure of information from student records maintained by school systems. Offered in the Senate by the distinguished and learned Senator from New York, James L. Buckley, this amendment, known as the Family Educational Rights and Privacy Act of 1974, is now law and became effective yesterday.

I regard the consideration of this bill today—the first comprehensive privacy bill to be reported by a House committee—as an indication both of the actual need for the protections embodied within it and of the growing awareness among legislators of that need.

THE PRIVACY ACT OF 1974

The bill before us, the Privacy Act of 1974, injects a new sensitivity to individual rights into all the recordkeeping practices of the Federal Government.

These fair information practices assert that there should be no recordkeeping system whose existence is a secret; that personal information in all files should be accurate, complete, relevant and up to date; that individuals should be able to review and correct almost all Federal files about themselves; that information gathered for one purpose should not be used for another without the individual's consent; and that the security and confidentiality of personal files should be assured.

The adoption of these rules as Federal policy is of historic dimensions.

In amending title 5, Government organization and employees, of the United States Code, to reflect these rules, the following specific requirements would be given force of law:

Permits an individual to have access to records containing personal information on him kept by Federal agencies, for purposes of inspection, copying, supplementation and correction—with certain exceptions, including law enforcement and national security records.

Allows an individual to control the transfer of personal information about him from one Federal agency to another for nonroutine purposes by requiring his prior written consent.

Makes known to the American public the existence and characteristics of all personal information systems kept by every Federal agency.

Prohibits the maintenance by Federal agencies of any records concerning the political and religious beliefs of individuals unless expressly authorized by law or an individual himself.

Limits availability of records containing personal information to agency employees who need access to them in the performance of their duties.

Requires agencies to keep an accurate accounting of transfers of personal records to other agencies and outsiders and make such an accounting available, with certain exceptions to the individual upon his request.

Requires agencies, through formal rulemaking, to list and describe routine transfers and establish procedures for access by individuals to records about themselves, amending records, handling medical information, and charging fees for copies of documents.

Makes it incumbent upon an agency to keep records with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in making determinations about him.

Provides a civil remedy by individuals who have been denied access to their records or whose records have been kept or used in contravention of the requirements of the act. The complainant may recover actual damages and costs and attorney fees if the agency's infraction was willful, arbitrary, or capricious.

Makes unlawful possession of or disclosure of individually identifiable information by a government employee punishable by a fine not to exceed $5,000.

Provides that any person who requests or obtains such a record by false pretenses is subject to a fine of not to exceed $5,000.

And, sets forth statutory provisions relating to archival records; requires annual report from President on agency uses of exemptions; and provides that the law would become effective 180 days following enactment.

On the whole, these are the recommendations arising from the initial protection of privacy bill introduced this Congress, the Goldwater-Koch-Kemp bill, particularly as those recommendations relate to access, inspection, copying, supplementation, and correction of records.

The few problems associated with the bill reported by the Committee are susceptible, I believe, to remedy through the amendment process this afternoon.

PRIVACY OF MEDICAL RECORDS AND MEDICAL INFORMATION

Subsection (f)(3) of the proposed section 552a of title 5 would require that each agency maintaining a system of records to promulgate rules to establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him.

The committee's report clarifies this section with the following language:

> If, in the judgment of the agency, the transmission of medical information directly to a requesting individual could have an adverse effect upon such individual, the rules which the agency promulgates should provide means whereby an individual who would be adversely affected by receipt of such data may be apprised of it in a manner which would not cause such adverse effects. An example of a rule serving such purpose would be transmission to a doctor named by the requesting individual.

As one who is particularly concerned with the right of privacy as it pertains to medical records and information—those records and that information held by the Federal agencies as well as those held within the States—I am encouraged by the direction of the committee's action in this regard. But, more should be done.

It is for that reason that I introduced, on October 11, the bill, H.R. 17323, to establish a Federal Medical Privacy Board with responsibility for promoting protection of the right of privacy as it relates to personal medical information.

That bill would establish a comprehensive, mandatory program of protection of the confidentiality of medical records held by Federal agencies and would establish a financial assistance program to States which develop adequate programs for the protection of non-Federal records, held by Government or within the private sector, in their respective States.

This subject is too serious—and potentially too far-reaching—to be dealt with as just one of many items to be covered by a more comprehensive act. I support, as I indicated earlier, the provision in the bill now before us as to medical records, but I do not feel it is adequate. Neither do I feel that amendments to that section which will be offered this afternoon—although I may support them because they do enhance this section of the bill—can adequately deal with this issue. Only the enactment of a comprehensive measure, like that contained in the proposed Medical Records Privacy Act, is required.

H.R. 17323 was introduced for the expressed purpose of soliciting the views of those to be affected by it—patients, hospital administrators, doctors, associations, insurance companies, attorneys, et cetera. Those comments are now coming in, and they will add immeasurably in the preparation of a perfected bill before the end of the session.

Mr. DRINAN. Mr. Chairman, this bill and the right to privacy have been long aborning. Over 80 years ago, Samuel Warren and Louis Brandeis published their seminal article on "The Right to Privacy" in the Harvard Law Review. In exalting the "right to be let alone," they identified the need to insulate from outside instrusion the "sacred precincts of private and domestic life."

Warren and Brandeis predicted that the "question whether our law will recognize and protect the right to privacy must soon come before our courts for consideration." The expectation that the judiciary would secure these rights has not been fully realized. To be sure, the courts have ventured into the area to some degree. But the judicial attempts to protect privacy have been slow and uneven. They have not been adequate to meet the concerns of contemporary society, partly because technology has outdistanced the common law and partly because Government has outdistanced the common man.

The present need for legislation is quite plain. Through the unceasing efforts of Chairman Moorhead, Congressman Koch, and others, the Privacy Act of 1974 is now before us. As a cosponsor of earlier versions of this bill and a participant in the drafting process through its principal sponsors, I have a particularly keen interest in it.

H.R. 16373 deals with a subject in which I have regularly expressed concern over the years. In the first days of my service in the House, I spoke to this body on the pernicious effects generated by the record-keeping activities of the Internal Security Committee. That practice and other recordations about the lives of our citizens continue on a daily basis by the agencies of the U.S. Government. Personal data which find their way into Government files often find their way out and into the hands of others.

The Privacy Act of 1974 seeks to arrest and control the dissemination of information already collected and stored. It does not purport to regulate the flow of data into Government files nor does it seek to affect the storage of such material. In this analytical sense it is a

limited measure. But its importance cannot be overstated. Providing access for persons to examine their files and restricting the distribution of the information contained in them should receive the highest commendation.

H.R. 16373 is a major step in regulating individual files maintained by the Government. It would give individuals access to their files, allow copies to be made, and permit corrections to be inserted. The bill restricts access to records by agency employees on a "need-to-know" basis. Federal workers who could not demonstrate that threshold requirement would be prohibited from examining individual records. The bill would also severely limit the transfer of files from one agency to another. Finally it would require the agency to record the names of all persons who are given access to a person's file.

The bill also provides civil remedies and criminal penalities for violations of its commands. A person who has been aggrieved by agency action may bring suit in the United States District Court to correct any unlawful practice. During the course of that litigation, the district judge is authorized by section (g)(2)(A) to review de novo any determination by an agency, for example, that a record should be withheld. In deciding the case, the judge may order an in camera inspection to make sure that the agency, in refusing to disclose a record, has complied with the law.

These provisions for de novo review and in camera inspection of documents are extremely important. Because of them, the agency cannot hide behind an executive classification which seeks to place the file beyond the reach of the citizen and the Federal court. Under this section, the judge may require any agency, including the Central Intelligence Agency and law enforcement authorities, to produce the records in question for his examination to determine if they are properly within the scope of the claimed exemption.

It may be, for example, that an executive agency might seek to conceal some of its records by transferring them to the CIA for safekeeping. If those files were then sought by an individual, the CIA would undoubtedly resist turning them over to that person. If a suit were then instituted to compel disclosure, the judge could order the records produced for his in camera inspection to determine whether they were in fact CIA records exempted by the statute. In essence this provision achieves the same result as H.R. 12471, the Freedom of Information Act amendments, which we recently passed. In that bill, we included a similar section to overturn the decision of the Supreme Court in *Environmental Protection Agency* v. *Mink*, 410 U.S. 73 (1973). Section (g)(2)(A) of this bill has an identical thrust.

There are, to be sure, provisions in this bill which should give us pause. The general exemptions for the Central Intelligence Agency and for law enforcement authorities are unwarranted and unnecessary. There is no provision for the establishment of a Federal privacy board which was in the predecessor bill, H.R. 667. The 180-day delay in the effective date of this bill could reasonably be cut in half. But even so, it is still a good proposal.

The recent inquiry by this House into the office of the President disclosed a number of practices which invade the privacy of American citizens. By regulating the manner in which Government agencies

conduct their business, as this bill does, we take another important step in protecting the "sacred precincts of private and domestic life." H.R. 16373 does not guarantee that abuses will no longer occur, but it does place checks upon those who could exercise power improperly. I urge my colleagues to vote in favor of this measure.

Mr. MOAKLEY. Mr. Chairman, the bill that was brought before us today was a landmark piece of legislation. It was an essential first step toward the protection of every American's right to privacy.

Unfortunately, the bill on which we are about to vote is no longer such a landmark. We have reneged on our promise to the American people that we would pass legislation to protect the right of every individual to privacy.

We have exempted Federal employees from the protections offered in the provisions of this bill, and we have allowed those Federal agencies afraid to conduct their business in the light of day to continue to work under a cloak of secrecy.

I am voting for this bill, but I do so with the sincere hope that when we return in January as the 94th Congress we will keep the promise that we have made. I, for one, will continue to fight for strong legislation in the area of privacy.

We must establish through legislation an agency with direct oversight of privacy statutes and regulations.

We must reconsider the exceptions to this law, and we must severely narrow those exemptions.

I deeply regret that I cannot offer my wholehearted support for this legislation, legislation which in its former strong and comprehensive state supported every step of the way since coming to Congress.

Mr. KOCH. Mr. Chairman, the first privacy legislation on the subject matter covered by the legislation on the floor today was the bill H.R. 7214 which I introduced on February 19, 1969. There is no legislation in which I have been involved here in the Congress that has given me greater satisfaction and a sense of accomplishment than this. The bill before us does not contain all of the safeguards that I would like to see in privacy legislation. I have some differences with respect to some provisions of the bill, but I do believe the bill to be one well worth supporting.

The basic weaknesses as I see them have to do with several areas. The bill is deficient in the area covering law enforcement agencies. However, that comes about because the House Judiciary Committee under the subcommittee chairmanship of DON EDWARDS is considering comprehensive legislation covering the entire criminal justice field. The Senate provision of the comparable bill which covers this particular area is preferable and yet that too is deficient when compared to the needs. Until the Justice Department can come forward with a proposal that the Congress can agree upon, criminal justice systems should be included in this privacy legislation. It would be completely unjustifiable to exempt criminal justice systems. Privacy legislation must affect law enforcement records. What is significant is section 3(e)(4) of the bill which applies to agency requirements which states that no agency, including law enforcement agencies, is permitted to maintain a record concerning the political or religious beliefs or activities of any individual unless expressly authorized by statute or by the individual himself.

The exemptions section should be limited only to those files having to do with national defense and foreign policy, information held pursuant to an active criminal investigation, and records maintained for statistical purposes not identifiable to an individual. I regret that the amendment to allow court assessment of punitive damages failed in a vote, and I also regret that the Erlenborn amendment to withhold from an individual the source of confidential information in his file carried.

There is one other area which is included in the Senate bill and that is the establishment of a Federal Privacy Commission which I hope will ultimately be incorporated in the final bill. Key to the concept of enforcing this privacy legislation, insuring the individual's privacy and the Federal agencies' carrying out of this function, is a Privacy Commission. Rather than fight the battle at this point, I would prefer that the legislation before us with its imperfections is sent to conference with the Senate, is perfected there and voted out before the 93d Congress adjourns. However, since the amendment to establish a Commission was voted down today, the House must be prepared to insure that the Commission's functions are absorbed in the privacy bill. The functions of the Commission are:

First, a directory of information systems;

Second, management of systems, oversight and privacy impact statements;

Third, research on the scope and effect of the systems; and

Fourth, an ombudsman role for the individual.

Basic to my 5-year effort to establish privacy standards for all Federal agencies has been the requirement that a directory of data banks be published and available to the general public. Provisions to this effect were part of the bipartisan measure which Congressman Goldwater and I introduced in April. Most regrettably, H.R. 16373 as reported contains no specific provision for the publication of a directory of the existence and character of personal systems of records in the executive branch. This can be remedied by minor changes to the agency notice and rule requirements sections of the bill.

The present agency requirements simply call for the annual noticing in the Federal Register of the existence and character of the systems of personal records together with important particulars about the location, categories of information, purpose, policies, practices address and procedures for notification and access. Under agency rules, all rules promulgated to carry out the requirements of the act, in compliance with section 553 of title 5 on rulemaking and public comment, must be published in the Federal Register and made available to the public. This language fails to require the publication of the character of each personal register with these rules. Therefore the public would not have any indication as to the different information systems to which they refer.

I understand there have been objections to an annual catalog of data banks by persons who claim it would be an unwieldy series of volumes. If a separate publication for agency rules were produced there would be two extensive documents. Convenience, uniformity, and likelihood of the general public's use of this information would be impaired. The cost might be prohibitive. As far as I know the so-called unworkability

factor, duplication, and cost are the only OMB reasons for opposing a directory.

In an effort to learn the true operating situation, the mechanics of preparing and publishing such directories, I have consulted with officials of the Federal Register. Strangely, mine was the first inquiry from Congress about how to sort out these questions and see that H.R. 16373 is written in a prudent, clear form. These discussions provided me with several important conclusions:

First. An annual directory is not necessary once the basic catalog is published, after that annual updatings can be printed to list changes in registers or note totally new ones.

Second. The language providing for agency notice requires so much detail on procedures for access and notification, policies for storage and practices over such things as disposal of records, that this overlaps significantly into the rule-making area. It would be impractical to separate the notice requirement and agency rules requirement, therefore they should be printed in the Federal Register concurrently and published in a directory in similar form.

Third. For the original implementation of reporting requirements, it would be wise to involve the Administrative Committee on Federal Reports composed of the Archivist, Attorney General, Public Printer with the Director of the Federal Register serving as its secretary. This committee could prepare a model notice and rule formats for the agencies thus helping to assure uniformity and consistency in presentation. Experience with the reports requirement of the Freedom of Information Act proves that a meaningful public document will need expert advice by the officials represented on this committee.

Mr. Chairman, I offered an amendment so an efficient and economical Directory of Federal Data Banks will be required in the Privacy Act of 1974. We cannot succeed in protecting privacy with a code of fair information practices which does not call for a publicly available directory of personal registers.

I do feel that any agency establishing a new data system or substantially changing an existing one should obtain from the National Bureau of Standards an assessment of that system's security safeguards and that the agency should report on this to the Office of Management and Budget and the Congress.

With no Privacy Commission in the House bill, we must be concerned with how the function that the Commission would have performed by way of assessing the privacy impact of systems will be taken care of. The National Bureau of Standards should be consulted with and given an assessment of the security safeguards.

My office has consulted with NBS on this issue. NBS has the authority to issue standards and under the Brooks legislation, NBS with OMB does have input in regards to the procurement of data systems. However, at the present time it is totally permissive for agencies to come to the NBS for technical safeguard assessment before the agency launches new personal information systems. In fact, NBS has yet to be called in on one new start. This was particularly dramatic in the case of the FEDNET plan, advanced by GSA. We should specify that NBS should perform this assessment function, particularly in the area of security safeguards.

Doug Metz, deputy executive director of the Domestic Council Committee on the Right of Privacy has said that one of the task force recommendations made to the committee has been that the Federal Government establish policies and procedures to insure the establishment of privacy safeguards in new telecommunications and data processing systems or substantial modifications to existing systems. OMB is now clearing with Government agencies interim guidelines for such privacy screening.

Agencies should report on the security safeguards to the Congress and OMB prior to the establishment of a new system. In this way we will avoid the situation of another FEDNET being contemplated and the Congress not knowing until the proposal has reached the appropriation stage. At the moment there is no proper way in the early stages of a contemplated system for Congress to be notified. I see no reason why a similar report as the one now formally required by agencies for OMB cannot be furnished the Congress. Without such advance notice, in the preapproval stage, Congress will be left to search the Federal Register and may be relegated to commenting on new or modified systems, rather than to stop or redirect them.

Contained in all measures I have introduced to protect individual records and require open-access practices, is the establishment of a board to regulate, monitor, and hear public grievances. H.R. 16373 contains no privacy agency and leaves individuals largely adrift if they need assistance or wish to protest inability to exercise access or other rights to their personal records. The Senate bill does have a board exercising this function which I favor.

I have looked into the Office of Consumer Affairs possible role as an "ombudsman" for privacy complaints as Mrs. Knauer's office serves in the consumer protection area. Aside from good work in developing and circulating a code of fair information practices for retail stores and other businesses, the Office of Consumer Affairs is not well equipped with statutory authority, technical competence, or access to operating agencies.

This vacuum must be filled and I am hopeful that a Privacy Commission having these duties will prevail. The legislative history must indicate a public repository for assistance and complaints on compliance with data protection standards.

Congress has been plagued by lack of information on problems involving technology and practices of State and private personal records systems. No research dimension is called for in the House bill. In the Senate measure a well-formulated research program is provided. We are told that the Domestic Council Committee on Right to Privacy is now doing much of this job. That is fine. But Congress and the American people cannot be expected to rely on a temporary committee operating under the nonstatutory Domestic Council, at the behest of the sitting President, in the purview of regularly exercised executive privilege. While I have a high regard for the committee, the fact is they cannot give Congress assurance that the reports and background documents related to their several studies will be made public.

Mr. Chairman, I bring up these deficiencies, along with the need for clear language authorizing a directory, as constructive suggestions for consideration.

I am particularly proud of the fact that this legislation moved ahead in the year of the 93d Congress because it received across the board political support. It became known initially as the Koch and Goldwater privacy bill. And, while it might have seemed strange to some that Koch and Goldwater could join together on some piece of legislation, those who understand the basic premise of conservative and liberal ideology appreciate the fact that on the issue of privacy there is a commonality of interest and concern. The bill before us is the work product of a great number of persons on the committee.

However, I again want to take special note of the enormous support and efforts that subcommittee Chairman William Moorhead and Congresswoman Bella Abzug gave in shaping the legislation, on the Democratic side in committee, as did all the members on that committee. And I also especially want to thank the ranking minority members, John Erlenborn and Frank Horton who worked so diligently to bring this legislation to the floor. The bipartisanship shown was reflected in the Government Operations Committee vote when it passed the bill out of committee 39 to 0. I also want to give special thanks to Senators Ervin, Percy, Bayh, Muskie, and Ribicoff for their efforts on the Senate side, which side is today considering companion legislation.

I shall now list the major areas that the bill covers:

First, it permits an individual to gain access to a file held on him by any Federal agency;

Second, permits any person to supplement the information contained in his file;

Third, permits the removal of erroneous or irrelevant information and provides that agencies and persons to whom the erroneous or irrelevant material has been previously transferred, be notified of its removal;

Fourth, prohibits records from being disclosed to anyone outside a Federal agency, except on an individual's request and when permitted by this act in some specified cases;

Fifth, requires an agency to inform an individual of his or her rights when supplying information to the agency;

Sixth, requires an agency to publish notice in the Federal Register of the existence of any system of records held by that agency so that no system will be secret;

Seventh, requires an agency to set rules for access to records, describe the routine uses of the records, establish procedures whereby an individual can amend his record, keep an accurate accounting of disclosures, and keep records in a timely, relevant and accurate manner;

Eighth, prohibits an agency from maintaining a record of political and religious beliefs or activities on an individual, unless expressly authorized by statute or by the individual himself;

Ninth, provides for certain exemptions for CIA files, law enforcement files, secret service files and statistical reporting systems; and

Tenth, provides for a civil remedy for an individual who has been denied access to his records, or whose record has been maintained and used in contravention of this act and an adverse effect results.

Mr. Ashbrook. Mr. Chairman, I have long had an intense interest in the issue of privacy. In 1962 I introduced a bill to curb the brain-picking tests being given to our Nation's school children. All too often

these psychological tests constituted an outright invasion of the privacy of the home and family life. Therefore my bill specifically required that parents be apprised of tests of a nonacademic nature which are administered to their children.

More recently, I helped enact the Buckley-Ashbrook amendment to the Elementary and Secondary Education Amendments of 1974. This amendment denies funds to school districts that do not restrict outside access to student records. It also gives parents and students in higher education the right of access to their files.

The threat of government intrusion into the lives and privacy of individuals has particularly grown during the past 40 years. During that time liberal politicians have consistently promoted a large Federal Government as the solution to all of our Nation's problems. It is somewhat ironic that liberals are now discovering that big government can also create problems.

A prime example of this is the area of individual privacy. As the Federal Government has grown in power, it has increasingly intruded into the personal lives of its citizens.

Particularly disturbing is the vast amount of personal information that is being collected and stored by the various Federal agencies. This information, which is usually hidden from the individual's view, is subject to great abuse. With the advent of computer technology and the ability to store almost unlimited amounts of data, the potential threat has become all the greater.

The bill before us—H.R. 16373—is necessary to reduce that threat. It estabishes safeguards to help prevent the misuse of personal information by the Federal Government.

Specifically, H.R. 16373 will in most cases allow an individual to see and correct the personal information that is kept on him by Federal agencies. It will also require an individual's prior written consent before personal information can be transferred from one Federal agency to another. Furthermore, agencies must make public the existence of all personal information systems. These and other safeguards provided for in this bill will help reassure the right of personal privacy for our Nation's citizens.

I am proud to support this legislation and I urge its adoption.

Mr. Broomfield. Mr. Chairman, privacy is a right long cherished by Americans and inherent in the Constitution and the Bill of Rights. But, as events in the last decade have shown, there is a tremendous need to enact legislation that will guarantee the ability of all American citizens to determine who will have knowledge of their own private lives. H.R. 16373, the privacy bill of 1974, is an enormous step forward toward meeting this need and I am proud to be a cosponsor of this legislation.

Approximately three out of every four Americans have part of their life histories recorded in computed data banks throughout the country, 7,000 of which are operated by the Federal Government. Yet no Federal law currently exists which permits citizens access to these files in order that they may insure the accuracy of the personal information that is contained on them. Neither can an individual control the transfer of personal information from agency to agency or even to people totally outside the Federal Government.

The implications of this lack of regulation are terrifying. The specter of 1984 has been raised so often that for some, it seems only a scare tactic. But the case of a 16-year-old schoolgirl provides otherwise. Because of a misaddressed letter that was sent to an organization on which the FBI had placed a mail-cover, Lori Paton became the subject of an FBI investigation. Fortunately, she was able to obtain destruction of her file through court action, but others may not be so lucky.

H.R. 16373 is a crucial start toward guaranteeing that other Americans will not undergo experiences similar to those of Lori Paton. The provisions of H.R. 16373 provide basic safeguards of personal privacy to the American people. At the same time, the framework of law it creates to protect the individual does not interfere unduly with the legitimate need of the Government for information about individuals in order to perform its required functions.

The Privacy Act of 1974 has grown from a series of intensive hearings and studies by the House Foreign Operations and Government Information Subcommittee and was approved unanimously. Its support is broad based and bipartisan. I urge all my colleagues to support this bill so that the assurance of all Americans to what Justice Holmes called "the right most valued by civilized men" can be strengthened under law.

Mr. DON H. CLAUSEN. Mr. Chairman, I rise in strong support of H.R. 16373.

The bill, as its name so rightly indicates, is for the purpose of insuring a higher degree of privacy for the individual. It establishes much-needed standards for the collection, maintenance, and dissemination of personally identifiable records maintained by Federal agencies and permits the individual access to these records and an opportunity to correct errors in them.

The need to protect the individual's right to privacy has become increasingly more important with the expanded use of interconnected computer systems and has been exemplified by an alarming increase in the number of abuses.

In particular, I wholeheartedly support the effort being led by my distinguished colleague from California (Mr. GOLDWATER) to prohibit a person from being required to disclose his or her social security number for any purpose not related to the operation of the social security program. I am a cosponsor of this proposal.

A limitation on the use of the social security number is necessary to protect the individual from the impersonal data banks which can threaten his right to privacy of information about his activities, his finances, and his lifestyle in general. The prohibition will not prevent the accumulation of such information but it will make the exchange of the information between computers much more difficult than it is at the present time when nearly everyone is asked to include his social security number on nearly every form he fills out.

Social security numbers were originally for the exclusive use of the social security people, looking out for each person's individual equity and benefits. Now it has reached the point where computers talk to computers, and the potential invasion of a person's entire private life has become a matter of grave concern to the people.

This legislation is an important step forward in our fight to secure the right of privacy for the individual and I urge my colleagues to support it. It is too easy for government to intimidate, harass or monitor the individual—we must end this possibility in whatever way we can. The adoption of this bill, as amended, is really striking a blow for freedom and the retention of our cherished privacy. I am pleased and proud of the Congress' efforts to advance and accept our legislative proposal.

Mr. GOLDWATER. Mr. Chairman, I am proud and pleased to state to my colleagues in the House that the Republican Task Force on Privacy played an important part in the successful enactment of the Privacy Act of 1974. It is therefore fitting that the product of their investigations be a part of the proceedings:

(BY HOUSE REPUBLICAN RESEARCH COMMITTEE, RECOMMENDATIONS OF PRIVACY TASK FORCE)

The House Republican Research Committee has approved the following recommendations of the Task Force on Privacy which deal with the following areas: Government Surveillance, Federal Information Collection, Social Security Numbers/Standard Universal Identifiers, Census Information, Financial Information, Consumer Reporting, School Records, Juvenile Records, Arrest Records, Medical Records, Computer Data Banks, Code of Ethics.

The House Republican Task Force on Privacy believes that the right to privacy is an issue of paramount concern to the nation, the public and the Congress. Recently publicized incidents of abuses have begun to focus attention on this long neglected area. Public awareness must be heightened and the legislative process geared up to address the full range of problems posed by the issue.

Modern technology has greatly increased the quantity and detail of personal information collection, maintenance, storage, utilization and dissemination. The individual has been physically by-passed in the modern information process. An atmosphere exists in which the individual, in exchange for the benefit or service he obtained, is assumed to waive any and all interest and control over the information collected about him. On the technical and managerial levels, the basic criteria in many decisions relating to personal information practices are considerations of technological feasibility, cost-benefit and convenience. The right to privacy has been made subservient to concerns for expediency, utility and pragmatism.

The trend in personal information practice shows no signs of abating. Twice as many computer systems and seven times as many terminals—particularly remote terminals—will be in use by 1984 as are in use today. And, with each federal service program that is initiated or expanded, there is a geometrically proportionate increase in the quantity and detail of personal information sought by the bureaucracy. The theory is that the broader the information base, the more efficient and successful the administration of the program.

Such a situation demands the attention of Congress and of the American public. The computer does not by definition mean injury to individuals. Its presence has greatly contributed to the American economy and the ability of government to serve the people. Under present procedures, however, the American citizen does not have a clearly defined right to find out what information is being collected, to see such information, to correct errors contained in it, or to seek legal redress for its misuse. Simply put, the citizen must continue to give out large quantities of information but cannot protect himself or herself from its misappropriation, misapplication or misuse. Both government and private enterprise need direction, because many of their practices and policies have developed on an isolated, ad hoc basis.

The House Republican Task Force on Privacy has investigated the following general areas involving the investigation and recording of personal activities and information: government surveillance, federal information collection, social security numbers and universal identifiers, census information, bank secrecy, consumer reporting, school records, juvenile records, arrest records, medical records, and computer data banks. These inquiries have resulted in the develop-

ment of general suggestions for legislative remedies. Each statement is accompanied by a set of findings.

All findings and recommendations are presented with the intent of being consistent with these general principles:

1. There should be no personal information system whose existence is secret;
2. Information should not be collected unless the need for it has been clearly established in advance;
3. Information should be appropriate and relevant to the purpose for which it has been collected;
4. Information should not be obtained by illegal, fradulent, or unfair means;
5. Information should not be used unless it is accurate and current;
6. Procedures should be established so that an individual knows what information is stored, the purpose for which it has been recorded, particulars about its use and dissemination, and has the right to examine that information;
7. There should be a clearly prescribed procedure for an individual to correct, erase or amend inaccurate, obsolete, or irrelevant information;
8. Any organization collecting, maintaining, using, or disseminating personnel information should assure its reliability and take precautions to prevent its misuse;
9. There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent;
10. The Federal Government should not collect personal information except as expressly authorized by law; and
11. That these basic principles apply to both governmental and non-governmental activities.

Each recommendation of the Task Force seeks to contribute to a broader, more intelligent, viable understanding of the need for a renewed concern for personal privacy. An awareness of personal privacy must be merged with the traditional activities of the free marketplace, the role of government as a public servant, and the need for national security defense, and foreign affairs.

SURVEILLANCE

The Task Force is deeply distributed by the increasing incidence of unregulated clandestine government surveillance based solely on administrative or executive authority. Examples of such abuses include wiretapping, bugging, photographing, opening mail, examining confidential records and otherwise intercepting private communications and monitoring private activities. Surveillance at the federal level receives the most publicity. However, state and local government, military intelligence and police activities also must be regulated.

The Fourth Amendment of the Constitution clearly specifies "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." The First Amendment guards against abridgement of the rights of free speech, free press, and assembly for political purposes. The Fourteenth Amendment states that none of a citizen's rights may be taken from him by governmental action without the due process of law.

The direct threat to individual civil liberties is obvious in those cases in which a person is actually being monitored, but even more alarming is the "chilling effect" such activities have on all citizens. A person who fears that he will be monitored may, either subconsciously or consciously, fail to fully exercise his constitutionally guaranteed liberties. The mere existence of such fear erodes basic freedoms and cannot be accepted in a democratic society.

The various abuses of discretionary authority in the conduct of surveillance provide ample evidence that current safeguard mechanisms do not work. Procedures allowing the executive branch to determine whether a surveillance activity is proper or not pose certain conflict of interest questions.

A degree of controversy surrounds the question of the authority of the President to initiate electronic surveillance without the safeguards afforded by court review. Present law is clear on this point: the Omnibus Crime Control and Safe Streets Act of 1968 lists those specific crimes in connection with which electronic monitoring may be instituted and requires that court approval be obtained in these cases. However, dispute has arisen over Executive claims of Constitutional prerogatives to implement wiretaps for national security purposes. The Supreme Court has ruled that, if such prerogative exists, it does not apply

to cases of domestic surveillance unrelated to national security. The Court has not yet ruled on the constitutionality of national security wiretaps unauthorized by a court. Cases are pending before the courts at this time which raise this issue. The Task Force agrees with the movement of the Judiciary to circumscribe unauthorized wiretaps and hopes it will proceed in this direction.

The Task Force feels that the surveillance is so repugnant to the right to individual privacy and due process that its use should be confined to exceptional circumstances. The Task Force further feels that no agent of federal, state, or local government should be permitted to conduct any form of surveillance, including wiretapping of U.S. citizens in national security cases, without having demonstrated probable cause and without having obtained the approval of a court of competent jurisdiction. The Task Force recommends enactment of new legislation to prohibit the unauthorized surveillance by any means, and further recommends that existing laws be clarified to the extent this may be necessary to ensure that no agent of the government, for any reason, shall have the authority to conduct any surveillance on any American citizen for any reason without first obtaining a court order.

The Task Force believes that this proposal would not lessen the capability of the government to protect and defend the American people, but would go a long way toward assuring the individual citizen that his constitutional rights will not be abridged by government without due process of law.

FEDERAL INFORMATION COLLECTION

Recently, there has been a pronounced increase in federal data and information collection. Over 11.5 million cubic feet of records were stored in Federal Records Centers at the beginning of FY 1973. Accompanying this increase has been a rise in the potential for abuse of federal information collection systems.

The Federal Reports Act of 1942 was enacted to protect individuals from overly budensome and repetitive reporting requirements. The agency entrusted with the responsibility for implementing the Act has ignored the legislative mandate and failed to hold a single hearing or conduct any investigations. With the exception of the Bureau of the Census and the Internal Revenue Service, there are few restrictions on the collection or dissemination of confidential information compiled by federal agencies.

The Task Force recommends that the Office of Management and Budget immediately begin a thorough review and examination of all approved government forms and eliminate all repetitive and unnecessary information requirements.

Legislation setting down clear guidelines and spelling out restrictions is needed to protect the individual from unrestricted and uncontrolled information collection: Individuals asked to provide information must be apprised of its intended uses. Individuals supplying information which will be made public must be notified of that fact at the time the information is collected or requested. Public disclosure (including dissemination on an intra- or inter-agency basis) of financial or other personal information must be prohibited to protect the privacy of respondents.

Returning the use of the Social Security Number (SSN) to its intended purpose (i.e. operation of old-age, survivors, and disability insurance programs) is a nessary corollary to safeguarding the right of privacy and curtailing illegal or excessive information collection.

The use of the Social Security Number has proliferated to many general items including state driver licenses, Congressional, school and employment identification cards, credit cards and credit investigation reports, taxpayer identification, military service numbers, welfare and social services program recipients, state voter registration, insurance policies and records and group heatlh records.

There are serious problems associated with the use of the SSN as a standard universal number to identify individuals. A standard universal identifier (SUI) will relegate individuals to a number; thereby, increasing feelings of alienation. The SSN's growing use as an identifier and filing number is already having a negative, dehumanizing effect upon many citizens. In addition, the use of a SUI by all types of organizations enables the linking of records and the tracking of an individual from cradle to grave. The possibility would negate the right to make a "fresh start", the right of anonymity, and the right to be left alone, with no compensating benefit.

A well-developed SUI system would require a huge, complex bureaucratic apparatus to control it and demand a strict system of professional ethics for information technicians. The technology needed to protect against unauthorized use has not yet been adequately researched and developed. A loss, leak or theft would seriously compromise a system and official misappropriation could become a political threat. The following Congressional action is needed:

1. legislation should be enacted that sets guidelines for use of the SSN by limiting it to the operation of old-age, survivors, and disability insurance programs or as required by federal law;

2. any Executive Orders authorizing federal agencies to use SSN's should be repealed, or alternatively, reevaluated and modified;

3. legislation should be enacted restricting the use of the SSN to well-defined uses, and prohibiting the development and use of any type of SUI until the technical state of the computer can ensure the security of such a system. At that time, a SUI system should have limited applicability and should be developed only after a full congressional investigation and mandate; and

4. new government programs should be prohibited from incorporating the use of the SSN or other possible SUI. Existing programs using the SSN without specific authorization by law must be required to phase out their use of the SSN. State and local governmental agencies, as well as the private sector, should follow this same course of action.

A review should be conducted of the Internal Revenue Service in both its collection and dissemination policies. Leaks must be ended. The need for stricter penalties for unauthorized activities should be reviewed.

CENSUS BUREAU

The greatest personal data collection agency is the Bureau of Census. Created to count the people in order to determine congressional districts, this agency has mushroomed into a vast information center which generates about 500,000 pages of numbers and charts each year.

Under penalty of law, the citizen is forced to divulge intimate, personal facts surrounding his public and private life and that of the entire family. These answers provide a substantial personal dossier on each American citizen. The strictest care must be taken to protect the confidentiality of these records and ensure that the information is used for proper purposes.

The Census Bureau sells parts of its collected data to anyone who wishes to purchase such information. Included are all types of statistical data that are available on population and housing characteristics. As the questions become more detailed and extensive, broadscale dissemination becomes more threatening and frightening. When used in combination with phone directories, drivers' licenses and street directories, census data may enable any one interested to identify an individual. Therefore, it is vitally important that rules and regulations governing the access to and dissemination of this collected data be reviewd, clarified and strengthened.

Legislation is needed to guarantee the confidentiality of individual information by expanding the scope of confidentiality under existing law and by increasing the severity of punishment for divulging confidential information. These provisions should be specifically directed at the officers and employees of the Bureau of Census, all officers and employees of the Federal government and private citizens who wrongfully acquire such information. In addition, the Bureau of the Census must use all available technological sophistication to assure that individuals cannot be inductively identified.

FINANCIAL INFORMATION

On October 26, 1970, sweeping legislation known as the Bank Secrecy Act became law. The Act's intention was to reduce white collar crime by making records more accessible to law enforcement officials. However, in accomplishing its purpose, it allowed federal agencies to seize and secure certain financial papers and effect of bank customers without serving a warrant or showing probable cause. The Act's compulsory recordkeeping requirements, by allowing the recording of almost all significant transactions, convert private financial dealings into the personal property of the banks. The banks become the collectors and custodians of financial records which, when improperly used, enable an individual's entire life style to be tracked down.

The general language of the Act allowed bureaucrats to ignore the intent of the law and neglect to institute adequate privacy safeguards. The Supreme Court affirmed this approach by upholding the consitutionality of both the law and the bureaucratic misinterpretation of it.

Congress must now take action to prevent the unwarranted invasion of privacy by prescribing specific procedures and standards governing the disclosure of financial information by financial institutions to Federal officials or agencies. Congress must enact legislation to assure that the disclosure of a customer's records will occur only if the customer specifically authorizes a disclosure or if the financial institution is served with court order directing it to comply. Legislation must specify that legal safeguards be provided requiring that the customer be properly notified and be provided legal means of challenging the subpena or summons.

Passage of such legislation would be an important step forward in reaffirming the individual's right to privacy.

CONSUMER REPORTING

The consumer reporting industry, through its network of credit bureaus, investigative agencies, and other reporting entities is in growing conflict with individual privacy. Most Americans eventually will be the subject of a consumer report as a result of applying for credit, insurance, or employment. The problem is one of balancing the legitimate needs of business with the basic rights of the individual.

Consumer reports fall into two categories. First, there are the familiar which contain "factual" information on an individual's credit record such as where accounts are held and how promptly bills are paid. 100 million consumer reports are produced each year by some 2600 credit bureaus.

The second ones go beyond factual information to include subjective opinions of the individual's character, general reputation, personal characteristics, and mode of living. These are often obtained through interviews with neighbors, friends, ex-spouses and former employers or employees. An estimated 30 to 40 million such reports are produced annually.

The first Federal attempt at regulating the collection and reporting of information on consumers by third-party agencies came in 1970 with the enactment of the Fair Credit Reporting Act (FCRA). In theory, the Act had three main objectives: to enable consumers to correct inaccurate and misleading reports; to preserve the confidentiality of the information; and to protect the individual's right to privacy.

The specific safeguards provided by the FCRA are: A consumer adversely affected because of information contained in a consumer report must be so notified and given the identity of the reporting agency. The consumer is entitled to an oral disclosure of the information contained in his file and the identity of its recipients. Items disputed by the consumer must be deleted if the information cannot be reconfirmed. The consumer may have his version of any disputed item entered in his file and included in subsequent reports.

The FCRA needs to be strengthened in two major areas: disclosure requirements and investigative reports. The individual should be entitled to actually see and inspect his file, rather than rely on an oral presentation. Further, he should be allowed to obtain a copy of it by mail (the consumer is often geographically distant from the source of the file). Users of consumer reports should be required to specifically identify the information which triggered any adverse action.

The FCRA protects the sources used in investigative reports. The Task Force believes that this contrary to the basic tenets of our system of justice and that the information source must be revealed upon the subject's request. Furthermore, the Task Force recommends that advance written authorization be required from any individual who is the subject of an investigative report for any purpose.

SCHOOL RECORDS

The recent increase in popular awareness of the seriousness of the privacy issue has been accompanied by an increase in the general concern over loose, unstructured and unsupervised school recordkeeping systems and associated administrative practices. There has also been general discussion about what information should be kept on a child and considered part of his or her "record." Parents are frequently denied access to their own child's record, or are prohibited from

challenging incorrect or misleading information contained in his file. At the same time, incidents of highly personal data being indiscriminately disseminated to inquirers unconnected with the school system are not uncommon.

Remedial measures are available to the Congress in the form of legislative actions. The sanctions under which such provisions would operate, however, are the key to their effectiveness. The Task Force proposes the Congress adopt as a general policy the rule that federal funds be withheld from any state or local educational agency or institution which has the policy of preventing parents from inspecting, reviewing, and challenging the content of his or her child's school record. Outside access to these school records must be limited so that protection of the student's right to privacy is ensured. It is recommended that the release of such identifiable personal data outside the school system be contingent upon the written consent of the parents or court order.

All persons, agencies, or organizations desiring access to the records of a student must complete a written form indicating the specific educational need for the information. This information shall be kept permanently with the file of the student for inspection by parents of students only and transferred to a third party only with written consent of the parents. Personal data should be made available for basic or applied research only when adequate safeguards have been established to protect the students' and families' rights of privacy.

Whenever a student has attained eighteen years of age, the permission or consent required of and the rights accorded to the parents should be conferred and passed to the student.

Finally, the Secretary of HEW should establish or designate an office and review board within HEW for the purpose of investigating, processing, reviewing, and adjudicating violations of the provisions set forth by the Congress.

JUVENILE RECORDS

The Task Force supports the basic philosophy underlying the existence of a separate court system for juvenile offenders, which is to avoid the stigmatizing effect of a criminal procedure. The lack of confidentiality of such proceedings and accompanying records subverts this intent and violates the individual's basic right of privacy.

Most states have enacted laws to provide confidentiality. Yet the Task Force finds that due to a lack of specific legislation, and contrary to the intent of the juvenile justice system, the individual's right of privacy is often routinely violated. Juvenile records are routinely released to the military, civil service, and often to private employers as well. This occurs in cases in which the hearing involves non-criminal charges, in cases of arrest but no court action, in cases in which the individual is no longer under the jurisdiction of the juvenile court, and in cases where this file has been administratively closed.

Legislation governing the confidentiality of juvenile court and police records varies widely from state to state. Only 24 states control and limit access to police records, therefore enabling a potential employer who is refused access to court records to obtain the information from the police. Only 16 states have expungement laws providing for the destruction of such records after a specified period of good behavior. Only 6 states make it a crime to improperly disclose juvenile record information. And, one state, Iowa, in fact provides that juvenile records must be open to the public for inspection. The Task Force finds that even in those states whose laws provide adequate protection, actual practices are often inconsistent with legislation.

Many new questions about confidentiality, privacy and juvenile rights are being raised, and the Task Force finds that the establishment of safeguards has lagged significantly behind technological developments. For example, presently no state has enacted legislation regulating the use of computers in juvenile court; as a rule, each system establishes its own guidelines for data collection, retention, and distribution.

The Task Force finds that with the use of computers, the juvenile's right to privacy is additionally threatened by the increased accessibility to his record and therefore increased possibility of misuse. Staff carelessness, less than strict adherence to rules of limited access, and electronic sabotage must now be added to the existing threats to the juvenile's right to privacy.

The Task Force recommends the establishment of minimum federal standards for state laws to include the following provisions:

1. all records of the juvenile court and all police records concerning a juvenile shall be considered confidential and shall not be made public. Access to these records shall be limited to those officials directly connected with the child's treatment, welfare, and rehabilitation;

2. dissemination of juvenile records, or divulgence of that information for employment, licensing, or any purpose in violation of statutory provisions shall be subject to a criminal penalty;

3. to protect the reformed delinquent from stigma continuing into his adult life, provisions should specify a procedure for either the total destruction or the sealing of all juvenile court and police investigative and offender records at the time the youth reaches his majority, or when two years have elapsed since he has been discharged from the custody or supervision of the court. Subsequent to this expungement, all proceedings and records should be treated as though they had never occurred and the youth should reply as such to any inquiry concerning his juvenile record; and

4. all police records on juveniles arrested but where no court action was taken should be systematically destroyed when the incident is no longer under active investigation.

The Task Force recommends the enactment of legislation specifically prohibiting federal agencies from requesting information relating to juvenile record expungement from employment applicants or from requesting such information from the courts or the police.

The Task Force further recommends the cessation of all Federal funding for computerized systems which contain juvenile records unless it can be demonstrated that these systems provide adequate safeguards for the protection of the juvenile's right of privacy. These standards must fulfill all the requirements of the minimum standards for state legislation previously enumerated, including special provisions to strictly limit data accessibility.

ARREST RECORDS

A large percentage of arrests never result in conviction. Yet, in over half the states, individual's arrest records are open to public inspection, subjecting innocent parties to undue stigma, harassment, and discrimination.

Persons with arrest records often find it difficult, if not impossible to secure employment or licenses. A study of employment agencies in the New York City area found that seventy-five percent would not make a referral for any applicant with an arrest record. This was true even in cases in which the arrest was not followed by a trial and conviction. This is just one example of the widespread practice of "presumption of guilt" based on the existence of an arrest record.

The Task Force holds that release of information about arrests not followed by conviction is a direct violation of the individual's rights of privacy. It therefore recommends that legislative efforts be directed toward:

1. establishing minimum standards for state laws calling for the automatic sealing of all individual arrest records which were not followed by conviction and which are no longer under active investigation;

2. requiring the FBI to seal arrest records not followed by convictions; and

3. prohibiting inclusion of arrest records not followed by conviction on computerized systems involving more than one state or using federal funds.

MEDICAL RECORDS

Medical records, which contain sensitive and personal information, are especially in need of privacy safeguards to maintain basic trust in the doctor-patient relationship. Yet, development of automated data processing systems has enhanced the ability of government and private organizations to store, analyze and transfer medical records. Increasingly, this occurs without the individual's knowledge or consent. Abuse of such information systems can have a deleterious effect on doctor-patient relations.

To guarantee the privacy of medical records, the Task Force recommends that:

1. the federal government provide dollar grants and incentives to States for the voluntary adoption and execution of State plans to insure the right to privacy for computerized medical information systems. Such a plan would place principal responsibility on the States, giving the federal government the right to set minimum standards;

2. Congress review the recently enacted Professional Standards Review Organizations (PSRO) legislation. There are increasing numbers of reports and complaints regarding Review Board uses of medical files and the threat this poses to privileged, confidential doctor-patient relationships; and

3. provisions be included in national health insurance legislation which specifically ensure the individual's privacy. The institution of a national health insurance plan will create a vast medical information network which will require stringent safeguards to prevent abuses of the patients' right to privacy.

COMPUTER DATA BANKS

The use of the computer has brought great commercial and social benefits to modern America. Greater reliance on the computer, however, increases its integration into all aspects of daily life. The result is increased vulnerability to abuse or misuse of computerized information.

The Task Force finds that the individual possesses inadequate remedies for the correction of such abuses. In fact, the Task Force considers it probable that many abuses have gone unreported simply because the individual involved did not know of the data being collected about him.

Even if the individual is aware that data is being collected about him, he faces several obstacles if he wishes to expunge purely private information or to correct erroneous information. Among his obstacles are the following: the lack of statutory support for legal action (except in the credit reporting area), the cost of litigation, and even fear of retaliation by the company or agency being challenged.

Despite their potential for abuse, data banks remain an inescapable fact of life in a society growing more complex and more technological. The Task Force does not oppose data banks as such, but favors strong safeguards against their misuse, and recommends that:

1. rights under the Fair Credit Reporting Act of 1970 be extended to all data collection. The individual must have and be informed of his right to review information in any collection of data about himself (excluding national security and criminal justice files);

2. Congress establish categories (i.e. indepth biographical, financial, medical, etc.) of information which may not be included in reports on an individual unless the individual knowingly gives his uncoerced consent;

3. limited exceptions be granted for national security and criminal justice investigations;

4. criminal and civil penalties be established for any use of statistical data (collected for collective analysis) to wrongfully acquire information on individuals;

5. transfer of personal information between governmental agencies be strictly limited;

6. the creation of a centralized Federal data bank (except for national security and criminal justice purposes) be prohibited; and

7. a federal "privacy protection agency" be established to enforce the proposed legislation.

CODE OF ETHICS AND STANDARD OF CONDUCT

The Republican Task Force on Privacy believes there to be a definite need for the development of a universal code of ethics and standard of conduct for the technical, managerial and academic personnel involved in the development and use of personal information systems. The Task Force regards this to be essential for the automated and computerized information systems. Personal information systems are becoming an integral aspect of the daily life of every individual in our society. This sensitive relationship demands and merits the development of an attitude of professionalism. It is recognized that some efforts have been made to develop and foster such attitudes. But, the information industry as a whole has not supported such efforts as a matter of policy. The Task Force declares its commitment to the development, maintenance, management and use of personal information systems.

CONCLUSION

The Task Force is aware that this is a relatively new area of concern. Some recommendations may go too far and some not far enough. Some areas may have been overlooked. But there is no question that now is the time to address our-

selves to this important and far reaching issue. If we fail—George Orwell's 1984 may become a reality by 1976.

BIBLIOGRAPHY

Breckenridge, Adam Carlyle, The right to privacy. Lincoln, University of Nebraska Press, 1970.

Canada. Department of Communication and the Department of Justice. Privacy and computers. A report of a task force established jointly by the Canadian Department of Communication and the Department of Justice. Ottawa, Canada, Information Canada, 1972.

Campaign, Howard and Lance J. Hoffman. Computer privacy and security. Computers and automation, v. 22, July 1973.

Cashman, Charles E. Confidentiality of juvenile court proceedings: A review. Juvenile Justice, v. 24, August 1973.

Cohen, Richard E. Justice report/hearings focus on privacy, limitations on use of FBI data. National journal reports, Feb. 16, 1974.

Computer applications in the juvenile justice system, National Council of Juvenile Court Judges, 1974.

Countryman, Vern. The diminishing right of privacy: The personal dossier and the computer. *Texas Law Review*, May 1971.

Curran, William J., et al., Protection of privacy and confidentiality, Science, v. 182, Nov. 23, 1973.

De Weese, J. Talyor. Giving the computer a conscience, Harper's, Nov. 1973.

Gotlieb, Calvin. Regulations for information systems. Computers and automation, v. 19, Sept. 1970.

Gough, Aidan R. The expungement of adjudication records. Washington University Law Quarterly, 1966.

Hunt, M. K. and Rein Turn. Privacy and security in data bank systems: an annotated bibliography. 1969–1973. R–1044–NSF. Santa Monica, Calif., Rand Corp., 1974.

Hoffman, Lance J. Security and privacy in computer systems. Los Angeles, Calif., 1973.

Hoglund and Kahan. Invasion of privacy and the freedom of information act: German v. NLRB, 40 Geo. Washington Law Review, 1972.

Koehn, E. Hank. Privacy, our problem for tomorrow. Journal of Systems management, v. 24, July 1973.

Kraning, Alan. Wanted: new ethics for new techniques. Technology review, v. 70, Mar. 1970.

Kuhn, David. Your life: how private? Reprint from Minneapolis Tribune, Oct. 7–12, 1973 by the Project on Privacy and Data Collection of the American Civil Liberties Union Foundation, Washington, D.C.

Lapidus, Edith J. Eavesdropping on trial. Rochelle Park, New Jersey, Hayden Book Co., 1974.

Levin, Eugene. The future shock of information networks. Astronautics and aeronautics, Nov. 1973.

Lusky, Louis. Invasion of privacy: a clarification of concepts. Columbia Law Review, v. 72.

Miller, Authur R. The assault on privacy: computers, databanks, and dossiers. Ann Arbor, University of Michigan Press, 1971.

Miller, Herbert S. The closed door. U.S. Dept. of Labor, 1972.

National Committee for Citizens in Education. Children, parents and school records. Columbia, Md., National Committee for Citizens in Education, 1974.

Organization for Economic Co-operation and Development. Toward central government computer policies. OECO Information Studies, 1973.

Pennock, J. Roland and John W. Chapman. Privacy. New York. Atherton Press, 1971.

Privacy in the First Amendment. The Yale Law Journal, June 1973.

Project Search Staff. Committee on Security and Privacy. Security and privacy considerations in criminal history information systems. Technical Report No. 2. Sacramento, Calif., Project Search, California Crime Technological Research Foundation, July 1970.

Ralston, Anthony G. Computers and democracy. Computers and automation, v. 22, April 1973.

Reed, Irving S. The application of information theory to privacy in data banks, Santa Monica, Calif., Rand Corp., 1973.

Rule, James B. Private lives and public surveillance. London, Allen Lane, 1973.
Sargent, Francis W. Centralized data banks—where public technology can go wrong. Astronautics and aeronautics, v. 11, Nov. 1973.
Schrag, Peter. Dossier dictatorship. Saturday Review, April 17, 1971.
Social Security Administration. Social Security Number Task Force: Report to the Commissioner. Department of Health, Education and Welfare, 1971.
Springer, Eric W. Automated medical records and the law. Pittsburgh, Aspen Systems Corporation, 1971.
Stone, Michael and Malcolm Warner. The data bank society: organizations, computers, and social freedom. London, George Allen and Unwin LTD, 1970.
Thomas, Uwe. Computerized data banks in public administration. Paris, France, Organization for Economic Co-operation and Development, 1971.
Turn, Rein. Privacy and security in personal information databank systems. Prepared for the National Science Foundation. R–1044–NSF. March 1974. Santa Monica, Calif., Rand Corp., 1974.
U.S. Congress. House. Committee on Government Operations. Federal information systems and plans—Federal use and development of advanced technology. Hearings before the Subcommittee on Foreign Operations and Government Information. 93rd Cong. 1st and 2d session. Washington, U.S. Govt. Printing Office, 1973, 1974.
U.S. Congress. Senate. Committee on the Judiciary. Federal data banks, computers and the Bill of Rights. Hearings before the Subcommittee on Constitutional Rights. 92nd Cong. 1st session, Washington. U.S. Govt. Printing Office, 1971.
U.S. Department of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. Records, computers, and the rights of citizens. Washington, U.S. Govt. Printing Office, 1973.
Westin, Alan F. and Michael A. Baker. Databanks in a free society: computers, record-keeping, and privacy. Report of the project on Computer Databanks of the Computer Science and Engineering Board. National Academy of Science. New York, Quadrangle Books, 1972.
Wheeler, Stanton. On record: files and dossiers in American life. New York, Russell Sage Foundation, 1969.

The CHAIRMAN. Are there any further amendments? If not, the question is on the committee amendment in the nature of a substitute, as amended.

The committee amendment in the nature of a substitute, as amended, was agreed to.

The CHAIRMAN. Under the rule, the Committee rises.

Accordingly the Committee rose; and the Speaker having resumed the Chair (Mr. Brademas) Chairman of the Committee of the Whole House on the State of the Union, reported that that Committee having had under consideration the bill H.R. 16373 to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, pursuant to House Resolution 1419, he reported the bill back to the House with an amendment adopted by the Committee of the Whole.

The SPEAKER. Under the rule, the previous question is ordered.

Is a separate vote demanded on any amendment to the committee amendment in the nature of a substitute adopted in the Committee of the Whole? If no, the question is on the amendment.

The amendment was agreed to.

The SPEAKER. The question is on the engrossment and third reading of the bill.

The bill was ordered to be engrossed and read a third time, and was read the third time.

The SPEAKER. The question is on the passage of the bill.

The question was taken; and the Speaker announced that the ayes appeared to have it.

Mr. ERLENBORN. Mr. Speaker, I object to the vote on the ground that quorum is not present and make the point of order that a quorum is not present.

The SPEAKER. Evidently a quorum is not present.

The Sergeant at Arms will notify absent Members.

The vote was taken by electronic device, and there were—yeas 353, nays 1, not voting 80, as follows:

[Roll No. 641]

YEAS—353

Abdnor	Byron	Erlenborn
Abzug	Carney, Ohio	Esch
Adams	Carter	Evins, Tenn.
Addabbo	Casey, Tex.	Fascell
Alexander	Cederberg	Findley
Anderson, Calif.	Chamberlain	Fish
Anderson, Ill.	Chisholm	Fisher
Andrews, N.C.	Clark	Flood
Andrews, N. Dak.	Clausen, Don H.	Flowers
Annunzio	Clawson, Del.	Flynt
Archer	Cleveland	Foley
Arends	Cochran	Ford
Ashley	Cohen	Forsythe
Badillo	Collier	Fountain
Bafalis	Collins, Ill.	Fraser
Baker	Collins, Tex.	Frelinghuysen
Barrett	Conlan	Frenzel
Bauman	Conte	Frey
Beard	Conyers	Fulton
Bennett	Corman	Fuqua
Bevill	Cotter	Gaydos
Biaggi	Coughlin	Gettys
Biester	Cronin	Gibbons
Bingham	Culver	Gilman
Blackburn	Daniel, Dan	Ginn
Blatnik	Daniel, Robert W., Jr.	Goldwater
Bolling	Davis, Ga.	Gonzalez
Bowen	Davis, S.C.	Goodling
Brademas	Davis, Wis.	Gray
Bray	de la Garza	Green, Oreg.
Breckinridge	Delaney	Green, Pa.
Brinkley	Dellenback	Griffiths
Broomfield	Dellums	Gross
Brotzman	Denholm	Gubser
Brown, Calif.	Dennis	Gude
Brown, Mich.	Derwinski	Gunter
Brown, Ohio	Dickinson	Guyer
Broyhill, N.C.	Dingell	Haley
Broyhill, Va.	Donohue	Hamilton
Buchanan	Dorn	Hammerschmidt
Burgener	Downing	Hanley
Burke, Fla.	Drinan	Hanna
Burke, Mass.	Duncan	Hanrahan
Burleson, Tex.	du Pont	Hansen, Idaho
Burlison, Mo.	Eckhardt	Harrington
Burton, John	Edwards, Ala.	Hawkins
Burton, Phillip	Edwards, Calif.	Hechler, W.Va.
Butler	Eilberg	Heinz

Helstoski
Henderson
Hicks
Hinshaw
Holifield
Holt
Holtzman
Horton
Hosmer
Howard
Huber
Hudnut
Hungate
Hutchinson
Ichord
Jarman
Johnson, Calif.
Johnson, Colo.
Johnson, Pa.
Jones, Okla.
Jones, Tenn.
Jordan
Kazen
Kemp
Ketchum
King
Koch
Kyros
Lagomarsino
Leggett
Lehman
Lent
Litton
Long, La.
Long, Md.
Lott
Lujan
McClory
McCloskey
McCollister
McCormack
McDade
McEwen
McFall
McKay
McKinney
Macdonald
Madden
Madigan
Mahon
Mallary
Mann
Maraziti
Martin, Nebr.
Martin, N.C.
Mathias, Calif.
Mathis, Ga.
Matsunaga
Mayne
Mazzoli
Meeds
Melcher
Mezvinsky
Michel
Milford
Miller
Mills
Minish
Mink
Mitchell, Md.
Mitchell, N.Y.
Mizell
Moakley
Mollohan
Montgomery
Moorhead, Calif.
Moorhead, Pa.
Morgan
Mosher
Murphy, Ill.
Murtha
Myers
Natcher
Nedzi
Nelsen
Nichols
Nix
Obey
O'Brien
O'Hara
O'Neill
Owens
Parris
Passman
Patten
Pepper
Perkins
Pettis
Peyser
Pickle
Pike
Preyer
Price, Ill.
Price, Tex.
Pritchard
Quie
Railsback
Randall
Rees
Regula
Reid
Reuss
Rinaldo
Roberts
Robinson, Va.
Robison, N.Y.
Rodino
Rogers
Roncalio, Wyo.
Rooney, Pa.
Rose
Rosenthal
Rostenkowski
Roush
Rousselot
Roy
Roybal
Ruppe
Ruth
Ryan
Sandman
Sarasin
Sarbanes
Satterfield
Scherle
Schneebeli
Schroeder
Seiberling
Shipley
Shriver
Shuster
Sisk
Skubitz
Slack
Smith, Iowa
Smith, N.Y.
Snyder
Spence
Stanton, J. William
Stanton, James V.
Stark
Steed
Steele
Steelman
Steiger, Ariz.
Steiger, Wis.
Stokes
Stratton
Stubblefield
Stuckey
Studds
Sullivan
Symington
Talcott
Taylor, Mo.
Taylor, N.C.
Thompson, N.J.
Thompson, Wis.
Thone
Thornton
Towell, Nev.
Treen
Udall
Ullman
Van Deerlin
Vander Jagt
Vander Veen
Vanik
Veysey
Vigorito
Waggonner
Walsh
Wampler
Ware
Whalen
White
Whitehurst
Whitten
Widnall
Wiggins
Williams
Wilson, Bob
Wilson, Charles H., Calif.
Wilson, Charles, Tex.
Winn

Wolff	Yates	Young, Tex.
Wright	Yatron	Zablocki
Wyatt	Young, Alaska	Zion
Wydler	Young, Fla.	Zwach
Wylie	Young, Ill.	

NAYS—1

Landgrebe

NOT VOTING—80

Armstrong	Giaimo	Poage
Ashbrook	Grasso	Podell
Aspin	Grover	Powell, Ohio
Bell	Hansen, Wash.	Quillen
Bergland	Harsha	Rangel
Boggs	Hastings	Rarick
Boland	Hays	Rhodes
Brasco	Hébert	Riegle
Breaux	Heckler, Mass.	Roe
Brooks	Hillis	Roncallo, N.Y.
Burke, Calif.	Hogan	Rooney, N.Y.
Camp	Hunt	Runnels
Carey, N.Y.	Jones, Ala.	St Germain
Chappell	Jones, N.C.	Sebelius
Clancy	Karth	Shoup
Clay	Kastenmeier	Sikes
Conable	Kluczynski	Staggers
Crane	Kuykendall	Stephens
Daniels, Dominick V.	Landrum	Symms
Danielson	Latta	Teague
Dent	Luken	Tiernan
Devine	McSpadden	Traxler
Diggs	Metcalfe	Waldie
Dulski	Minshall, Ohio	Wyman
Eshleman	Moss	Young, Ga.
Evans, Colo.	Murphy, N.Y.	Young, S.C.
Froehlich	Patman	

So the bill was passed.

The Clerk announced the following pairs:

Mr. Hébert with Mr. Dulski.
Mrs. Boggs with Mr. Aspin.
Mr. Moss with Mr. Luken.
Mr. Sikes with Mr. McSpadden.
Mr. Boland with Mr. Young of Georgia.
Mr. Rooney of New York with Mr. Tiernan.
Mr. Giaimo with Mr. Traxler.
Mr. Staggers with Mr. Patman.
Mr. Hays with Mr. Minshall of Ohio.
Mr. Bergland with Mr. Kuykendall.
Mr. Chappell with Mr. Hunt.
Mr. Carey of New York with Mr. Hogan.
Mr. Brooks with Mr. Camp.
Mrs. Burke of California with Mr. Froehlich.
Mr. Breaux with Mr. Ashbrook.
Mr. Kluczynski with Mr. Grover.
Mr. Landrum with Mr. Devine.
Mr. Metcalfe with Mrs. Grasso.
Mr. Murphy of New York with Mr. Conable.
Mr. Teague with Mr. Hillis.
Mr. St Germain with Mr. Powell of Ohio.
Mr. Riegle with Mr. Bell.

Mr. Latta with Mr. Hastings.
Mr. Rangel with Mrs. Hansen of Washington.
Mr. Roe with Mr. Crane.
Mr. Jones of Alabama with Mr. Harsha.
Mr. Kastenmeier with Mr. Eshleman.
Mr. Karth with Mr. Clancy.
Mr. Jones of North Carolina with Mr. Quillen.
Mr. Diggs with Mr. Roncallo of New York.
Mr. Evans of Colorado with Mr. Sebelius.
Mr. Dent with Mr. Shoup.
Mr. Dominick V. Daniels with Mr. Stephens.
Mr. Clay with Mr. Waldie.
Mr. Danielson with Mr. Symms.
Mr. Runnels with Mr. Wyman.
Mr. Rhodes with Mr. Young of South Carolina.
Mrs. Heckler of Massachusetts with Mr. Rarick.

The Result of the vote was announced as above recorded.
A motion to reconsider was laid on the table.

[From the Congressional Record—House, Dec. 11, 1974]

HOUSE CONSIDERS S. 3418 AND SUBSTITUTES TEXT OF H.R. 16373

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I ask unanimous consent to take from the Speaker's table the Senate bill (S. 3418) to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes, and ask for its immediate consideration.

The Clerk read the title of the Senate bill.

The SPEAKER. Is there objection to the request of the gentleman from Pennsylvania?

There was no objection.

The Clerk read the Senate bill.[1]

* * * * * * *

MOTION OFFERED BY MR. MOORHEAD OF PENNSYLVANIA

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I offer a motion.

The Clerk read as follows:

Mr. MOORHEAD of Pennsylvania moves to strike out all after the enacting clause of S. 3418 and insert in lieu thereof the text of the bill (H.R. 16373) to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, as passed by the House.

The motion was agreed to.

The Senate bill was ordered to be read a third time, was read the third time, and passed.

The title was amended so as to read: "to amend title 5, United States Code, by adding a section 52a to safeguard individual privacy from

---

[1] See p. 437.

the misuse of Federal records and to provide that individuals be granted access to records concerning them which are maintained by Federal agencies."

[From the Congressional Record—House, Dec. 18, 1974]

HOUSE CONSIDERS AND ADOPTS COMPROMISE AMENDMENTS WITH THREE TECHNICAL AMENDMENTS

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I ask unanimous consent to take from the Speaker's desk the Senate bill (S. 3418) to establish a Privacy Protection Commission to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes, with Senate amendments to the House amendments and concur in the Senate amendments with an amendment.

The Clerk read the title of the bill.

The Clerk read the Senate amendments.[1]

* * * * * * *

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I ask unanimous consent that the full text of S. 3418, containing the Senate amendments to the House amendments, be considered to read and printed at this point in the RECORD, and that the text of the House technical amendment being offered also be printed at the end thereof.

The SPEAKER. Is there objection to the request of the gentleman from Pennsylvania?

Mr. ERLENBORN. Mr. Speaker, reserving the right to object, and I do not intend to object, I would like to ask the chairman of the subcommittee to explain the Senate amendments for our colleagues.

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I will be most pleased to explain the Senate amendments and then will yield to the gentleman from Illinois for additional comments he or other Members may have on the privacy bill, or for questions concerning its provisions.

First, let me explain briefly the parliamentary situation. Both the House and the Senate passed privacy legislation on November 21. Our bill, H.R. 16373, was messaged over to the Senate the following day. The Senate measures, S. 3418, sponsored by the distinguished Senator from North Carolina, Mr. ERVIN, and a number of other distinguished Members of that body from both parties, was messaged to the House. The House bill was called up on November 22 in the Senate, and all after the enacting clause was stricken and the identical language of S. 3418, was substituted for the House language, and it was returned to the House. This meant, Mr. Speaker, that both of the House and Senate versions of the privacy bills were pending at the Speaker's desk—but both bills—S. 3418 and H.R. 16373—had the identical language of the Senate-passed bill.

Because of the lateness in the session and the pressures on Members of both bodies due to other pressing legislative business, we determined that it would not be possible to resolve the complex differences between

---

[1] See p. 497.

the two bills in a conference committee. Yet the sponsors and floor managers of the legislation on both sides firmly agreed that it was imperative that final action be taken on privacy legislation before the end of the Congress.

We thereupon agreed, Mr. Speaker, upon a parliamentary procedure which provided that the Senate bill, S. 3413, be taken from the Speaker's desk, be taken up by the House and repassed with the language of the House bill, H.R. 16373, as passed, substituted for all after the enacting clause and returned to the Senate for further action. This action was taken by me last Wednesday, December 11 (RECORD, pages H11661–H11666), and the Senate bill was returned to that body with the language of H.R. 16373, as passed on November 21, and the short title was also amended to reflect the House version.

Mr. Speaker, the other body has now repassed S. 3413 with a series of amendments—many technical and some substantive—which retain the basic thrust of the House version, but which include important segments of the Senate measure. These amendments were informally negotiated by the staffs of the House and Senate committees and are based on agreements between the principal sponsors of the privacy bills in the two bodies.

In calling up the bill for final action and clearance for White House action today, I am asking that the House concur in these amendments—which in my opinion preserve the basic framework of the House bill, but which make a number of significant strengthening changes in the privacy measure that were included in the Senate version. As Members will recall, President Ford specifically endorsed the provisions of H.R. 16373 in October, with the provision that the amendment offered by the gentleman from Illinois (Mr. ERLENBORN), relating to certain confidential investigative records be included in the bill. Such amendment was agreed to by the House on November 20, and is included in the version of the privacy bill now before us. Thus, Mr. Speaker, the bill now being considered here today has the full backing of the White House, and the Members of both parties in the House and the Senate who have had the responsibility of handling the measure in committee and on the floor.

Mr. Speaker, in its concurrence, the House of Representatives is clearing for final congressional action what will be known as the Privacy Act of 1974. This is truly an historic enactment. In effect, the Congress of the United States is acting in the finest sense to implement even further the Bill of Rights.

To my knowledge, this will be the first congressional action on a comprehensive Federal privacy law since the adoption of the fourth amendment to the Constitution. It is the solemn duty of the Congress, as well as the Supreme Court, to implement the spirit and letter of the Constitution.

Although this bill is limited to personal information on individuals contained in Federal records, I am sure it is only the first step to strengthen the right to privacy.

The operative parts of this legislation will go into effect in 9 months. In its birth, I would like to think we are helping America prepare for a grand bicentennial, rededicating ourselves to the fundamental principles of individual freedom and dignity which made this Nation great.

Mr. Speaker, I will insert at this point in the Record the text of an analysis prepared by staff of the major amendments added to the House bill in the other body:

ANALYSIS OF HOUSE AND SENATE COMPROMISE AMENDMENTS TO THE FEDERAL PRIVACY ACT

The establishment of a Privacy Protection Study Commission. Only the Senate bill provided for an oversight and study commission to assist in the implementation of the act and to explore areas concerned with individual privacy which have not been included in the provisions of this legislation. The compromise measure will establish a Privacy Protection Study Commission of seven members instead of the five provided in the Senate bill. Three of these members will be appointed by the President, two by the President of the Senate, and two by the Speaker of the House of Representatives.

It is intended that this commission, which will serve for a period of two years, will be solely a study commission. In that capacity it is hoped the commission can assist the Executive Branch and the Congress in their examination of Federal government activities and their impact on privacy as well as representatives of State and local governments and the private sector who are attempting to deal with this important problem.

The scope of the commission's study authority is outlined specifically within the legislation. In section 5(c)(2)(B), the commission is directed to examine certain issues which are not included in the compromise between the House and Senate bill, such as a requirement that a person maintaining mailing lists remove an individual's name upon request; the question of prohibiting the transfer of individually identifiable data from the Internal Revenue Service to other agencies and to State governments; a question of whether the Federal government should be liable for general damages occurring from a willful or intentional violation of the provisions of new section 552a(g)(1)(C) or (D) which this act creates; and the extent to which requirements for security and confidentiality of records maintained under this act should be applied to a person other than an agency.

The commission shall from time to time and in an annual report, report to the Congress and to the President on its activities, and it shall submit a final report of its findings two years from the date the members of the commission are appointed.

In addition, the commission is authorized to provide necessary technical assistance and prepare model legislation upon request for State and local governments interested in adopting privacy legislation. Strict standards and penalties are placed upon commission members and employees with regard to the handling and unlawful distribution of information about individuals which it receives in the course of carrying out its functions.

While the provisions of the rest of this act do not go into effect until 270 days from the date of enactment, the commission is authorized to go into effect immediately upon the appointment of its members in order that some of its work may be available to the Congress and the Executive Branch by the time the remainder of the legislation becomes effective.

ROUTINE USE

The House bill contains a provision not provided for in the Senate measure exempting certain disclosures of information from the requirement to obtain prior consent from the subject when the disclosure would be for a "routine use". The compromise would define "routine use" to mean: "with respect to the disclosure of a record, the use of such records for a purpose which is compatible with the purpose for which it was collected."

Where the Senate bill would have placed tight restrictions upon the transfer of personal information between or outside Federal agencies, the House bill, under the routine use provision, would permit an agency to describe its routine uses in the Federal Register and then disseminate the information without the consent of the individual or without applying the standards of accuracy, relevancy, timeliness or completeness so long as no determination was being made about the subject.

The compromise definition should serve as a caution to agencies to think out in advance what uses it will make of information. This act is not intended to impose

undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.

INFORMATION ON POLITICAL ACTIVITIES

The House bill tells agencies that they may not maintain a record concerning the political or religious beliefs or activities of any individual unless maintenance of the record would be authorized expressly by statute or by the individual about whom the record is maintained. The House bill goes on to provide that this subsection is not deemed to prohibit the maintenance of any record or activity which is pertinent to and within the scope of a duly authorized law enforcement activity.

The Senate bill constitutes a prohibition against agency programs established for the purpose of collecting or maintaining information about how individuals exercise First Amendment rights unless the agency head specifically determines that the program is required for the administration of a statute.

The compromise broadens the House provisions application to all First Amendment rights and directs the prohibition against the maintenance, use, collection, or dissemination of records. However, as in the House bill, it does permit the maintenance of those records which are expressly authorized by statute or by the individual subject, or are pertinent to or within the scope of an authorized law enforcement activity.

CONFIDENTIAL SOURCES OF INFORMATION

The compromise provision for the maintenance of information received from confidential sources represents an acceptance of the House language after receiving an assurance that in no instance would that language deprive an individual from knowing of the existence of any information maintained in a record about him which was received from a "confidential source." The agencies would not be able to claim that disclosure of even a small part of a particular item would reveal the identity of a confidential source. The confidential information would at the very least have to be characterized in some general way. The fact of the item's existence and a general characterization of that item would have to be made known to the individual in every case.

Furthermore, the acceptance of this section in no way precludes an individual from knowing the substance and source of confidential information, should that information be used to deny him a promotion in a government job or access to classified information or some other right, benefit or privilege for which he was entitled, otherwise if he should consequently bring legal action against the government and should base any part of its legal case on that information.

Finally, it is important to note that the House provision would require that all future promises of confidentiality to sources of information be expressed and not implied promises. Under the authority to prepare guidelines for the administration of this act it is expected that the Office of Management and Budget will work closely with agencies to insure that Federal investigators make sparing use of the ability to make express promises of confidentiality.

STANDARDS APPLIED TO DISSEMINATION OUTSIDE THE GOVERNMENT

H.R. 16373 requires that all records which are used by an agency in making any determination about an individual be maintained with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in the determination. S. 3418 goes much further and requires that agencies apply these standards at any time that access is granted to the file, material is added to or taken from the file, or at any time it is used to make a determination affecting the subject of the file.

The difference between these two measures represents a difference in philosophy regarding the handling of personal information. The Senate measure is designed to complement the requirement that agencies maintain only information which is relevant and necessary to accomplish a statutory purpose. The standard of

relevancy should be that statutory basis for an information program which is now set forth in (e)(1) of the compromise measure. By adopting this section, the Senate hoped to encourage a periodic review of personal information contained in Federal records as those records were used or disseminated for any purpose.

The House provision would have applied these important standards for maintenance of information in records at any time a determination is made about an individual. The House bill goes on to permit additional "routine uses" of information which may not rise to the threshold of an "agency determination" without requiring that the information be upgraded to meet these standards.

The compromise amendment would adopt the section of the House bill applying the standards of accuracy, relevance, timeliness and completeness at the time of a determination. It would add the additional requirement, however, that prior to the dissemination of any record about an individual to any person other than another agency, the sending agency shall make a reasonable effort to assure that the record is accurate, complete, timely, and relevant. This proviso was included because Federal agencies would be governed by a requirement to clean up their records before a determination is made and limited by a requirement to publish each routine use of information in the Federal Register, but the use of information by persons outside the Federal government would not be governed by this act. Therefore, agencies are directed to be far more careful about the dissemination of personal information to persons not governed by the enforcement provisions of this bill.

THE FREEDOM OF INFORMATION ACT AND PRIVACY

One difficult task in drafting Federal privacy legislation was that of determining the proper balance between the public's right to know about the conduct of their government and their equally important right to have information which is personal to them maintained with the greatest degree of confidence by Federal agencies. The House bill made no specific provision for Freedom of Information Act requests of material which might contain information protected by the Privacy Act. Instead, in the committee report on the bill, it recognized that:

"This legislation would have an effect on subsection (b)(6) of the Freedom of Information Act (5 U.S.C., Section 552) which states that the provisions regarding disclosure of information to the public shall not apply to material 'the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.' H.R. 16373 would make all individually identifiable information in government files exempt from public disclosure. Such disclosure could be made available to the public only pursuant to rules published by agencies in the Federal Register permitting the transfer of particlar data to persons other than the individuals to whom they pertain."

The committee report went on to express a desire that agencies continue to make certain individually identifiable records open to the public because such disclosure would be in the public interest.

The Senate bill provided that nothing in the act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder. This section was intended as specific recognition of the need to permit disclosure under the Freedom of Information Act.

The compromise amendment would add an additional condition of disclosure to the House bill which prohibits disclosure without written request of an individual unless disclosure of the record would be pursuant to Section 552 of the Freedom of Information Act. This compromise is designed to preserve the status quo as interpreted by the courts regarding the disclosure of personal information under that section.

A related amendment taken from the Senate bill would prohibit any agency from relying upon any exemption contained in Section 552 to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

CIVIL REMEDIES

Under the House bill an individual would be permitted to seek an injunction against an agency only to produce his record upon a failure of an agency to comply with his request. An individual would be able to sue for damages only if an agency failed to maintain a record about him with such accuracy, rele-

vance, timeliness and completeness as would be necessary to assure fairness and a determination about him, and consequently an adverse determination was made. A suit for damages would also be in order against an agency if it fails to comply with any other provision of this act in such a way to have an adverse effect on the individual.

Under the Senate bill injunctive relief would be available to an individual to enforce any right granted to him. And an individual would be permitted to sue for damages for any action or omission of an officer or employee of the government who violates a provision of the act.

The standard for recovery of damages under the House bill was a determination by a court that the agency acted in a manner which was willful, arbitrary, or capricious. The Senate bill would have permitted recovery against an agency on a finding that the agency had erred in handling his records.

These amendments represent a compromise between the two positions. They permit an individual to seek injunctive relief to correct or amend a record maintained by an agency. In a suit for damages, the amendment reflects a belief that a finding of willful, arbitrary, or capricious action is too harsh a standard of proof for an individual to exercise the rights granted by this legislation. Thus the standard for recovery of damages was reduced to "willful or intentional" action by an agency. On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed as only somewhat greater than gross negligence.

Both the House and Senate bills provided for an individual to recover reasonable attorney fees and costs of litigation. The compromise amendments adopt the standard of the House bill permitting the court to award attorney fees and reasonable costs to an individual where a complainant has substantially prevailed in an injunctive action, and requiring such award in actions in which complainants receive damages.

ACCESS AND CHALLENGE TO RECORDS

The House bill would apply a standard of promptness to agency considerations of requests for access to records and requests to challenge or correct those records. In addition, it allows the individual to request a review of a refusal to correct a record by the agency official named in its public notice of information systems.

The Senate bill requires the agency to make a determination with respect to an individual's request for a record change within 60 days of the request and to permit him a hearing within 30 days of a request for one, with extension for good cause permitted. The individual would have the option of a formal or informal hearing procedure within the agency upon a refusal of a request to correct or amend a record. The compromise amendment would require the agency to respond within 10 working days to acknowledge an individual's request to amend a record. Following acknowledgement, the agency must promptly correct the information which the individual believes is not accurate, relevant, timely or complete or inform the individual of its refusal.

If the individual disagrees with the refusal of the agency to amend his record, the agency shall conduct a review of that refusal within 30 working days, provided that an extension may be obtained for good cause. We expect that agency heads will either conduct such reviews themselves, or assign officers of the rank of deputy assistant secretary or above.

The House bill would not have permitted a Federal District Court to review *de novo* an agency's refusal to amend a record. The compromise adopts the Senate provision which would require a *de novo* review of such refusal and to order a correction where merited. Finally, the compromise requires that in any disclosure of information subject to disagreement that the agency includes with the disclosure a notation of any dispute over the information or a copy of any statement submitted by the individual stating his reasons for disagreement with the information.

ACCOUNTING FOR DISCLOSURES

The House bill requires an agency to inform any person or another agency about a correction or notation of dispute regarding a record that has been disclosed to that person or agency within two years before making the correction or notation. It would not apply if no accounting of the disclosure had been required. No such limitation was placed upon accounting for disclosures in the

Senate bill and the compromise measure would require any person or agency receiving the record at any time before a notation or dispute is made to be notified if an accounting of the disclosures were made.

The House bill requires an agency to maintain an accounting for disclosures for only five years. The Senate bill places no limitation on the length of time for maintaining such disclosures. The compromise amendment would require maintaining of the disclosure for five years or the life of the record, whichever is longer.

LIMITATIONS ON THE TYPES OF INFORMATION COLLECTED AND THE USE OF THIRD PARTY INFORMATION

The Senate bill requires Federal agencies to maintain only such information about an individual as is relevant and necessary to accomplish a statutory purpose of the agency. The House bill did not address this issue. The compromise amendment modifies the Senate provision to permit the collection of information which would be required to accomplish not only a purpose set out by a statute but also a purpose outlined by a Presidential Executive Order.

The provision is included to limit the collection of extraneous information by Federal agencies. It requires that a conscious decision be made that the information is required to meet the lawful needs of an agency. Agencies should formulate as precisely as possible the policy objectives to be served by a data gathering activity before it is undertaken. It is hoped that multiple requests for information will be reduced and that agencies will collect no more sensitive personal information than is necessary.

The Senate bill also requires agencies to collect information to the greatest extent practicable directly from the subject when that information could result in an adverse determination about an individual's rights and benefits and privileges under a Federal program. The House bill had no provision, but the compromise amendment accepts the Senate language. This section is designed to discourage the collection of personal information from third party sources and therefore to encourage the accuracy of Federal data gathering. It supports the principle that an individual should to the greatest extent possible, be in control of information about him which is given to the government. This may not be practical in all cases for financial or logistical reasons or because of other statutory requirements. However, it is a principle designed to insure fairness in information collection which should be instituted wherever possible.

ARCHIVAL RECORDS

The House bill provides that records accepted by the Administrator of General Services for temporary storage and servicing shall be considered for purposes of this act, to be maintained by the agency which deposits the records. Records transferred to the National Archives after the effective date of this Act for purposes of historical preservation are considered to be maintained by the Archives and are subject only to limited provisions of the Act. Records transferred to the National Archives before the effective date of this Act are not subject to the provisions of this Act.

The Senate bill provides that records accepted by the Administrator of General Services for temporary storage and servicing shall be considered, for purposes of this Act, to be maintained by the agency which deposits the records. All records transferred to the National Archives for purposes of historical preservation are considered to be maintained by the Archives and are subject only to those provisions of this Act requiring annual public notice of the existence and character of the information systems maintained by the Archives, establishment of appropriate safeguards to insure the security and integrity of preserved personal information, and promulgation and implementation of rules to insure the effective enforcement of those safeguards.

The compromise amendment subjects records transferred to the National Archives for historical preservation prior to the effective date of the act to a modified requirement for annual public notice. It is intended that the notice provision not be applied separately and specifically to each of the many thousands of separate systems of records transferred to the Archives prior to the effective date of this Act, but rather that a more general description be provided which pertains to meaningful groupings of record systems. However, record systems transferred

to the Archives after the effective date of this Act are individually subject to the specific notice provisions. This coverage is intended to support and encourage improvements in the organization and cataloging of records maintained by the Archives.

MORATORIUM ON THE USE OF THE SOCIAL SECURITY ACCOUNT NUMBER

The House bill provides that a Federal agency, or a State or local government acting in compliance with Federal law or a federally assisted program, is prohibited from denying to individuals rights, benefits or privileges by reason of refusal to disclose the social security account number. Any such governmental agency is further prohibited from utilizing the social security account number for purposes apart from verification of individual identity except where another purpose is specifically authorized by law. Exempt from these prohibitions are systems of records in existence and operating prior to January 1, 1975. Exemption is further granted where disclosure of a social security account number is required by Federal law.

The Senate bill provides that a Federal agency, or a State or local government, is prohibited from denying to individuals rights, benefits or privileges by reason of refusal to disclose the social security account number. Persons engaged in the business of commercial transactions or activities are prohibited from discriminating against any individual in the course of such activities by reason of refusal to disclose the social security account number. Exempt from these prohibitions are systems of records in existence and operating prior to January 1, 1975. Also exempt are disclosures of the social security account number required by Federal law. This section further provides that any Federal, State or local government agency or any person who requests an individual to disclose his social security number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, what uses will be made of it, and what rules of confidentiality will govern it.

The compromise amendment changes the House language by broadening the coverage of State and local governments so as to prohibit any new activity by such a government that would condition a right, benefit or privilege upon an individual's disclosure of his social security account number.

To clarify the intent of the Senate and House, the grandfather clause of this section was re-stated to exempt only those governmental uses of the social security account number continuing from before January 1, 1975, pursuant to a prior law or regulation that, for purposes of verifying identity, required individuals to disclose their social security account number as a condition for exercising a right, benefit, or privilege. Thus, for illustration, after January 1, 1975, it will be unlawful to commence operation of a State or local government procedure that requires individuals to disclose their social security account numbers in order to register a motor vehicle, obtain a driver's license or other permit, or exercise the right to vote in an election. The House section was amended to include the Senate provision for informing an individual requested to disclose his social security account number of the nature, authority and purpose of the request. This provision is intended to permit an individual to make an informed decision whether or not to disclose the social security account number, and it is intended to bring recognition to, and discourage, unnecessary or improper uses of that number.

RULEMAKING PROCEDURES FOR MAKING EXEMPTIONS

To obtain an exemption from certain provisions of this Act under the House bill, agencies entitled to those exemptions would be required to public notice of the proposed exemptions in the *Federal Register* pursuant to Section 553 of the Administrative Procedures Act permitting comments to be submitted in writing for inclusion in the *Register* with such exemptions.

The Senate bill applied a much more stringent standard and would have required agencies to hold adjudicatory hearings as provided in APA Sections 556 and 557. The compromise agreements would no longer require full adjudicatory proceeding by any agency seeking an exemption permitted under the act. However, agencies would still be required to publish notice of a proposed rulemaking in the Federal Register and could not waive the 30 day period for such publication. In addition it is specifically provided in this act that agencies obtaining such exemptions state the reasons why the system of records is to be exempted.

DUTIES OF THE OFFICE OF MANAGEMENT AND BUDGET

Under the Senate bill the Privacy Protection Commission was directed to develop model guidelines and conduct certain oversight of the implementation of this Act to Federal agencies. Since the compromise amendment would change the scope of authority of the commission, it was felt there remained a need for an agency within the government to develop guidelines and regulations for agencies to use in implementing the provisions of the Act and to provide continuing assistance to and oversight of the implementation of the provisions of this Act by the agencies.

This function has been assigned to the Office of Management and Budget.

REPORTS ON NEW SYSTEMS

Under the Senate bill the Privacy Protection Commission was to have a central role in evaluating proposals to establish or alter new systems of information in the Federal government. If the commission had determined that such a proposal was not in compliance with the standards established by the Senate bill the agency which prepared the report could not proceed to establish or modify an information system for 60 days in order to give the Congress and the President an opportunity to review that report and the commission's recommendations.

The compromise amendment would require that agencies provide adequate advance notice to the Congress and to the Office of Management and Budget of any proposal to establish or alter a system of records in order to permit an evaluation of the privacy impact of that proposal. In addition to the privacy impact, consideration should be given to the effect the proposal may have on our Federal system and on the separation of powers among the three branches of government. These concerns are expressed in connection with recent proposals by the General Services Administration and Department of Agriculture to establish a giant data facility for the storing and sharing of information between those and perhaps other departments. The language in the Senate report on pages 64–66 reflects the concern attached to the inclusion of this language in S.3418.

The acceptance of the compromise amendment does not question the motivation or need for improving the Federal government's data gathering and handling capabilities. It does express a concern, however, that the office charged with central management and oversight of Federal activities and the Congress have an opportunity to examine the impact of new or altered data systems on our citizens, the provisions for confidentiality and security in those systems and the extent to which the creation of the system will alter or change interagency or intergovernmental relationships related to information programs.

GOVERNMENT CONTRACTORS

The Senate bill would have extended its provisions outside the Federal government only to those contractors, grantees or participants in agreements with the Federal government, where the purpose of the contract, grant or agreement was to establish or alter an information system. It addressed a concern over the policy governing the sharing of Federal criminal history information with State and local government law enforcement agencies and for the amount of money which has been spent through the Law Enforcement Assistance Administration for the purchase of State and local government criminal information systems.

The compromise amendment would not permit Federal law enforcement agencies to determine to what extent their information systems would be covered by the Act and to what extent they will extend that coverage to those with which they share that information or resources.

DEFINITION OF RECORD

The definition of the term "Record" as provided in the House bill has been expanded to assure the intent that a record can include as little as one descriptive item about an individual and that such records may incorporate but not be limited to information about an individual's education, financial transactions, medical history, criminal or employment records, and that they may contain his name, or the identifying number, symbol, or other identifying marks, particularly assigned to the individual, such as a finger or voice print or a photograph. The

amended definition was adopted to more closely reflect the definition of "personal information" as used in the Senate bill.

Mr. MOORHEAD of Pennsylvania. I will not take the time to explain each of these amendments because many of them are merely technical or conforming in nature. All of them are clearly germane to the original House bill. I will, however, mention the most important of them—

First, the bill provides for a seven-member Privacy Protection Study Commission, authorizing a 2-year study of various aspects of individual privacy affecting areas of the private sector and State and local governmental units. In my judgment, Mr. Speaker, such a study—without directly affecting the operational aspects of the Privacy Act of 1974—will be most helpful in understanding the complexities of individual privacy in non-Federal activities and in the consideration of additional legislation affecting privacy in the future.

Second, I would like to mention another amendment in the Senate bill that deals with mailing lists. Language included in the legislation would prohibit the sale or rental of mailing lists, names and addresses, by Federal agencies maintaining them. The philosophy behind this amendment is that the Federal Government is not in the mailing list business, and it should not be Federal policy to make a profit from the routine business of government, particularly when the release of such lists has been authorized under the Freedom of Information Act. In other words, such lists cannot be withheld by an agency, unless it determines that the release would constitute "a clearly unwarranted invasion of privacy" under section 552(b)(6) of title 5, United States Code.

Thus, the language of the bill before us does not ban the release of such lists where either sale or rental is not involved. Our subcommittee on Foreign Operations and Government Information held extensive hearings on Federal agency mail list policies during the last Congress. Such policy varies from agency to agency, and the Federal courts have interpreted in several cases the language of the Freedom of Information Act relating to withholding of matters constituting a "clearly unwarranted invasion of privacy." This measure now before us would preserve the current practices and interpretations of this part of the Freedom of Information Act, as they deal with Federal agency mailing lists.

Finally, the bill, as amended, assigns to the Office of Management and Budget the responsibility of developing guidelines and regulations for all Federal Agencies in the enforcement and administration of the Privacy Act.

Mr. Speaker, I will not discuss the other Senate amendments in any detail since a description of them has been placed in the Record previously. However, on the major areas of operational parts of the bill—such as access, accounting, disclosure, agency rules and requirements, and exemptions—the bill generally follows the House version. Some strengthening language has, however, been incorporated from the Senate measure.

Mr. Speaker, I now yield to the gentleman from Illinois (Mr. Erlenborn) who has made such a significant series of contributions at every stage in the development of this meaningful privacy legislation.

Mr. Speaker, some questions as to how the bill will work with respect to tax information and tax returns have arisen. Specifically, the questions relate to the ability of the IRS to disclose tax information under the provision of the bill that allows disclosure for a routine use under a purpose which is compatible with the purpose for which the information is collected.

State and local tax agencies now heavily rely on Federal tax information and investigations when State agencies enforce their tax laws. For example, when the IRS sets up a deficiency against a taxpayer who lives in a State, the IRS frequently sends information on this deficiency to the State or local tax agency. The States use this information in collecting their own taxes. This information may be sent before the State itself conducts any tax investigation on the individual.

Under the bill, this is intended to constitute a routine use for a purpose compatible with the purpose for which the information was collected, so the IRS could continue to send this information to the State and local tax agencies as is presently done.

Also, the IRS sends to State and local tax agencies the Federal tax returns of individuals who live in the State so the State agency can check to see if the individual has reported the same income and deductions on his Federal and State or local tax returns. Again, the States rely on this information in enforcing their own tax laws. Also, this information may be sent to a State before it conducts a tax investigation on its own.

Under the bill, it is intended that this would be a routine use for a purpose compatible with the purpose for which the information is collected so the IRS can continue to send tax information to State and local tax agencies in this way.

The IRS, of course, provides tax information on individuals to the Justice Department when the Justice Department is preparing a tax case against the individual. This information is used by the Justice Department in investigating and preparing tax cases and also is disclosed in court as the Justice Department presents evidence against the individual.

This disclosure both to the Justice Department and in court would represent a routine use of the tax information compatible with the purpose for which it was collected and this disclosure would continue to be possible under the provisions of the bill.

Under the bill tax returns and other tax information can—as under present law—be disclosed to the tax committees of the Congress: the Senate Finance Committee, the House Ways and Means Committee, and the Joint Committee on Internal Revenue Taxation.

Under the bill this information can also continue to be disclosed to the staffs of these committees, as under present law.

Under the bill an agency can disclose tax returns to either House of Congress or to committees of Congress to the extent of matters within their jurisdiction. Since tax returns can be disclosed by an agency to the Senate and House, it is intended that—as under present law—the committees which have received tax returns can also disclose them to the Senate or House, just as the Joint Committee on Internal Revenue Taxation did with the tax information on President Nixon.

Mr. Speaker, this bill deals with personal data that is frequently processed and stored on automated recordkeeping systems. These systems require the performance of appropriate maintenance techniques, for example memory dumps needed by nonagency personnel who diagnose and repair the equipment. How are these nonagency maintenance personnel to be viewed relative to the bill's disclosure and accounting provisions?

It is necessary to properly maintain recordkeeping systems in order to insure data accuracy and validity. It is our intention that authorized maintenance of automated systems performed by nonagency personnel be viewed as a legitimate extension of the authority of agency employees who must see personal data in the normal performance of their duties. Accordingly, nonagency personnel performing authorized maintenance would be in the same position as agency officials and employees.

Mr. ERLENBORN. Mr. Speaker, I withdraw my reservation of objection.

The SPEAKER. Is there objection to the request of the gentleman from Pennsylvania (Mr. Moorhead)?

There was no objection.

Mr. ALEXANDER. Mr. Speaker, when the House originally considered this bill, it adopted an amendment regarding certain investigatory material. I would ask the gentleman, does that amendment remain in the bill?

Mr. ERLENBORN. Yes, it does.

Mr. ALEXANDER. Exactly what does the amendment provide?

Mr. ERLENBORN. It says that the head of any agency may promulgate rules to exempt certain investigatory material from the access requirements of this legislation. Specifically, the material which may be exempted is, and I quote:

> Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

Mr. ALEXANDER. The amendment does not extend, then, to all investigatory material?

Mr. ERLENBORN. That is correct; it does not. It is limited in two important regards. First, it pertains only to investigatory material compiled solely for certain specified purposes. Second, and more important, it governs access to that information only to the extent that the disclosure of the material would reveal the identity of a confidential source.

Mr. ALEXANDER. Then this amendment would not permit an agency to withhold information which a confidential source gave to the agency.

Mr. ERLENBORN. That is correct. The agency would have to allow an individual access to all information regarding, let us say, his background security check, except the part which would reveal a confidential source. In some cases, this might be simply his name. This is far greater access than individuals have at the present time.

Mr. ALEXANDER. In some instances, I suppose, agencies might claim that disclosure of any part of a particular item would reveal the identity of a confidential source. In those instances, could the agencies conceal even the fact of the item's existence from the citizen who wished to see his file?

Mr. ERLENBORN. Absolutely not. The fact that a confidential derogatory statement exists in someone's file, and that the statement could be characterized in some general way, most assuredly would not reveal the identity of a confidential source. The fact of the item's existence and a general characterization of that item would have to be made known to the individual in every case.

Mr. ALEXANDER. Let me ask the gentleman one further question. Suppose an individual believed that he had not been promoted in his Government job because of confidential derogatory information in his file, and that the Government refused to allow the individual access to that information on the grounds that allowing access would reveal the identity of a confidential source. Suppose further that the individual then went to court and demanded that he be promoted, arguing that nothing on the public record interfered with his right to the promotion. Would the government then have to let him see the portion of his file which it had previously withheld?

Mr. ERLENBORN. If the Government wanted to introduce the statement into evidence in court, it would surely have to allow the individual to see the statement. If the Government had no other reason for denying the promotion, it would in effect have two choices: Release the information which would reveal the identity of the confidential source or lose the case.

Let me add one further thought here. We have been discussing for the past few minutes statements made by "confidential sources." The bill provides that with regard to statements made to Government agencies in the past, this term shall include all sources who furnished information under an implied promise that the identity of the source would be held in confidence. This is as it should be: we must protect the privacy of people who believe that they were speaking to Federal agents in a privileged fashion.

With regard to statements made to Government agencies in the future, however, the term will refer only to sources who furnish information under an express promise that the identity of the source would be held confidential. The Office of Management and Budget has assured us that it will issue guidelines and work closely with agencies to insure that Federal investigators make sparing use of the ability to make express promises of confidentiality. Both OMB and we want to insure that such promises are made only when the information involved is extremely important to the Government and would not be offered if the promises were not made in return.

Mr. ALEXANDER. I thank the gentleman for his remarks. I would like to turn briefly to the gentleman from Pennsylvania (Mr. Moorhead) and ask him if he concurs in the explanation of the amendment given by the gentleman from Illinois.

Mr. MOORHEAD of Pennsylvania. Mr. Speaker, I am happy to assure the gentleman that I am in complete agreement with the explanation.

Mr. HORTON. Mr. Speaker, I rise in support of this bill, which will add greatly to the protection of personal privacy of all Americans.

The bill achieves this objective by three means. First, it provides that citizens may have access to most records about them maintained by the Federal Government, and may request the Government to correct misstatements in the records. Second, it requires Federal agencies to make public all the uses they make of personal records, and forbids those agencies from transferring such records to persons not named in the published uses unless the individuals to whom the documents pertain have given their advance written consent to the transfers. Third, the bill allows citizens to file suit in Federal court to correct their records, see records about them which agencies withhold, and secure damages when they have been harmed by a willful or intentional action of an agency regarding their records.

Mr. Speaker, in writing H.R. 16373, the House bill which is very similar to the measure now before us, the Government Operations Committee, on which I serve as ranking minority member, made great efforts toward this end; as we added privacy protections for citizens, we did not want to add great burdens for Government agencies in implementing the bill. I think that we accomplished that goal by drawing the legislation so that agencies would have to publicize what they were doing, but would not have to submit to unreasonable requirements which would in effect prevent them from carrying out constructive programs.

The chairman of the Foreign Operations and Government Information Subcommittee, Mr. Moorhead of Pennsylvania, and the ranking minority member of that subcommittee, Mr. Erlenborn, have labored long and hard to insure that whatever bill eventually represented a synthesis of House and Senate measures on this subject be directed toward that same end. I commend them for their work; in my judgment, although the bill now before us includes some provisions from the Senate measure which I myself would not have proposed, those provisions are reasonable and the bill is a good one.

The major way in which this bill differs from the one passed by the House less than a month ago is that this legislation creates a Privacy Protection Study Commission to investigate the information practices of organizations of all kinds insofar as they relate to personal information, and recommend how individual privacy can best be protected, consistent with good recordkeeping practices. I hope that this Commission will make constructive recommendations and that they will lead to increased privacy for all Americans in the future. I expect that the Commission will use good sense in collecting information to be used in its study, and will, consistent with the spirit of this legislation, not interfere with the ongoing business of Government.

For example, the Congress has recognized in this bill that certain records, such as those maintained by the Central Intelligence Agency and others classified for national security reasons, should be exempt from the requirement that individuals have access to records about them. I trust that the Commission will conduct its affairs in such a way as not to impair the responsibility of the Director of the CIA to protect intelligence sources and methods or the head of any agency to keep classified documents secret.

Mr. Speaker, S. 3418 in its present form will help protect the personal privacy of our fellow Americans. I urge my colleagues to join me in supporting it.

Mr. Koch. Mr. Speaker, the first privacy legislation on the subject matter covered by the legislation on the floor today was the bill H.R. 7214 which I introduced on February 19, 1969. There is no legislation in which I have been involved here in the Congress that has given me greater satisfaction and a sense of accomplishment than this. The bill before us today, which earlier passed the House and Senate on November 21, is a good bill and one which I believe is well worth supporting. By its passage today we have reached a landmark in legislative history, and truly the 93d Congress can justly be called the privacy Congress.

I had hoped that a Federal Privacy Commission would ultimately be incorporated in the final bill. It was approved in the Senate, but not in the House. However, I am pleased that the compromise reached provided for at least a study commission of other governmental and private organizations. The study commission is directed to complete a report within two years and that report should include recommendations for applying privacy principles to those organizations being studied.

There is a basic missing provision not in the bill in the area covering law enforcement agencies. However, that comes about because the House Judiciary Committee under the subcommittee chairmanship of Don Edwards is considering comprehensive legislation covering the entire criminal justice field. It was and is my contention that until the Justice Department can come forward with a proposal that the Congress can agree upon, criminal justice systems should be included in this privacy legislation. It is completely unjustifiable to exempt criminal justice systems. Privacy legislation must affect law enforcement records. However, what is significant in the bill is a provision which states that no agency, including law enforcement agencies, is permitted to maintain a record concerning the political or religious beliefs or activities of any individual unless expressly authorized by statute or by the individual himself.

The exemptions section should have been limited only to those files having to do with national defense and foreign policy, information held pursuant to an active criminal investigation, and records maintained for statistical purposes not identifiable to an individual. I also regret that the provision to allow court assessment of punitive damages is not incorporated in this bill and that there is a provision to permit the withholding from an individual the source of confidential information in his file.

The bill does prohibit Federal agencies from selling or renting mailing lists except as authorized by law. Also, thanks to the enormous efforts of Barry Goldwater, Jr., there is a provision mandating that benefits not be denied to an individual solely for failure to disclose his social security account number, unless that disclosure is mandated by statute.

Basic to my 5-year effort to establish privacy standards for all Federal agencies has been the requirement that a directory of data banks be published and available to the general public. A provision I sponsored is in the bill providing for an efficient and economical Directory of Federal Data Banks. We cannot succeed in protecting privacy with a code of fair information practices unless there is a publicly available directory of personal information systems.

I am particularly proud of the fact that this legislation moved ahead in the year of the 93d Congress because it received across the board political support. It became known initially as the Koch and Goldwater privacy bill. And, while it might have seemed strange to some that Koch and Goldwater could join together on some piece of legislation, those who understand the basic premise of conservative and liberal ideology appreciate the fact that on the issue of privacy there is a commonality of interest and concern. The bill before us is the work product of a great number of persons on the committee.

However, I again want to take special note of the enormous support and efforts that subcommittee Chairman William Moorhead and Congresswoman Bella Abzug gave in shaping the legislation, on the Democratic side in committee, as did all the members on that committee. And I also especially want to thank the ranking minority members, John Erlenborn and Frank Horton, who worked so diligently to bring this legislation to the floor. The bipartisanship shown was reflected in the Government Operations Committee vote when it passed the bill out of committee 39 to 0. I also want to give special thanks to Senators Ervin, Percy, Bayh, Muskie, and Ribicoff for their efforts on the Senate side.

I shall now list the major areas that the bill covers:

First, it permits an individual to gain access to a file held on him by any Federal agency;

Second, permits any person to supplement the information contained in his file;

Third, permits the removal of erroneous or irrelevant information and provides that agencies and persons to whom the erroneous or irrelevant material has been previously transferred, be notified of its removal;

Fourth, prohibits records from being disclosed to anyone outside a Federal agency, except on an individual's request and when permitted by this act in some specified cases;

Fifth, requires an agency to inform an individual of his or her rights when supplying information to the agency;

Sixth, requires an agency to publish notice in the Federal Register of the existence of any system of records held by that agency so that no system will be secret;

Seventh, requires an agency to set rules for access to records, describe the routine uses of the records, establish procedures whereby an individual can amend his record, keep an accurate accounting of disclosures, and keep records in a timely, relevant and accurate manner;

Eighth, prohibits an agency from maintaining a record of political and religious beliefs or activities on an individual, unless expressly authorized by statute or by the individual himself;

Ninth, provides for certain exemptions for CIA files, law enforcement files, secret service files and statistical reporting systems; and

Tenth, provides for a civil remedy for an individual who has been denied access to his records, or whose record has been maintained and used in contravention of this act and an adverse effect results.

The legislation is far from perfect. It should be improved upon and expanded in its coverage in the 94th Congress. I believe that will occur as it did with Freedom of Information Act, and that the legislation

before us is a monumental breakthrough in the field of personal privacy safeguards.

The House amendment to the Senate amendments was agreed to.

The Senate amendments as amended were concurred in.

A motion to reconsider was laid on the table.

PART 4.—COMPLEMENTARY SPEECHES AND MATERIALS

[From the Office of the White House Press Secretary (Vail, Colorado), Jan. 1, 1975]

STATEMENT BY THE PRESIDENT UPON SIGNING OF THE PRIVACY ACT OF 1974

The Privacy Act of 1974, S. 3418, represents an initial advance in protecting a right precious to every American—the right of individual privacy.

I am especially happy to have signed this bill because of my own personal concern in the privacy issue. As Chairman of the Domestic Council Committee on the Right of Privacy, I became increasingly aware of the vital need to provide adequate and uniform privacy safeguards for the vast amounts of personal information collected, recorded and used in our complex society. It was my objective then, as it is today, to seek, first, opportunities to set the Federal house in order before prescribing remedies for State and local government and the private sector.

The Privacy Act of 1974 signified an historic beginning by codifying fundamental principles to safeguard personal privacy in the collection and handling of recorded personal information by Federal agencies. This bill, for the most part, strikes a reasonable balance between the right of the individual to be left alone and the interest of society in open government, national defense, foreign policy, law enforcement and a high quality and trustworthy Federal work force.

No bill of this scope and complexity—particularly initial legislation of this type—can be completely free of imperfections. While I am pleased that the Commission created by this law has been limited to purely advisory functions, I am disappointed that the provisions for disclosure of personal information by agencies make no substantive change in the current law. The latter in my opinion does not adequately protect the individual against unnecessary disclosures of personal information.

I want to congratulate the Congressional sponsors of this legislation and their staffs who have forged a strong bipartisan constituency in the interest of protecting the right of individual privacy. Experience under this legislation, as well as further exploration of the complexities of the issue, will no doubt lead to continuing Legislative and Executive efforts to reassess the proper balance between the privacy interests of the individual and those of society. I look forward to a continuation of the same spirit of bipartisan cooperation in the years ahead.

My Administration will act aggressively to protect the right of privacy for every American, and I call on the full support of all Federal personnel in implementing requirements of this legislation.

[From the Office of the White House Press Secretary, Washington, D.C., Sept. 29, 1975]

STATEMENT BY THE PRESIDENT ON THE IMPLEMENTATION OF THE PRIVACY ACT OF 1974

The Privacy Act of 1974 took effect on Saturday, September 27, 1975, a date marking a milestone in the protection of individual privacy for every American.

The reason this Act is important became apparent to me when I was Vice President and chairman of the Domestic Council Committee on the Right of Privacy. Last January, I was pleased to sign this bill as President because it represents a major first step in safeguarding individual privacy.

The need for a Privacy Act is manifestly clear: Over the years, Federal agencies have amassed vast amounts of information about virtually every American citizen. As data-collecting technology increased, it made administrative sense to combine much of this information in computerized data systems where it could be retrieved instantly at the push of a button. This fact in itself raised the possibility that information about individuals could be used for purposes outside the constraints of law and without the prior knowledge or consent of the individuals involved.

The worthwhile programs of human assistance for which this individual information is collected are vital to millions of Americans. They cannot be ended. But at the same time, we have a clear responsibility to erect reasonable safeguards to ensure that information collected is used solely for the purposes intended.

The Privacy Act, though experimental, makes a long overdue start to erect these safeguards. It requires Federal agencies to:

—Allow individuals to examine records pertaining to them and establish procedures for correcting those records;

—take steps to ensure the accuracy, timeliness and security of records that concern individuals and to limit records-keeping to necessary and lawful purposes.

This Act also provides special safeguards whenever the rights of citizens to free speech and expression are involved.

Before this Act, even the Federal Government did not know what information it kept about individuals. The Act, therefore, required Federal agencies to first inventory their records-keeping systems and identify those which contained information about individuals and to publish a listing of these systems in the Federal Register. That task is now complete.

The magnitude of Federal records-keeping has been far greater than anyone imagined. There are more than 6,000 Federal record systems containing personal data about them.

Compliance with this Act will involve many people. Every Federal official who either creates, keeps or uses personal data has responsibilities under this Act. I urge every member of the Executive Branch to reexamine the record systems in their custody and determine if all are necessary. Keeping only an essential minimum of these records is the most effective protection we have against further incursions by the Federal Government into the private lives of Americans.

AGENCY COMMENT FROM CENTRAL INTELLIGENCE AGENCY

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C., *September 26, 1974.*

Hon. SAM J. ERVIN, JR.,
Chairman, Committee on Government Operations,
U.S. Senate, Washington, D.C.

DEAR MR. CHAIRMAN: This is in response to a request from the staff of your Committee for views on a new Committee Print, No. 5, of S. 3418.

As explained in my letter to you of 23 July 1974 on S. 3418, certain information in the possession of this Agency must in the national interest remain confidential. The National Security Act of 1947 and the Central Intelligence Agency Act of 1949, have charged the Director of Central Intelligence with the responsibility for protecting Intelligence Sources and Methods from unauthorized disclosure (50 U.S.C.A. 403 (d)(3)) and exempted the Agency from provisions of law requiring public disclosures concerning organization, functions, names, titles, salaries, and numbers of personnel employed by the Agency (50 U.S.C.A. 403g).

The vast majority of this Agency's personal information holdings (foreign persons living abroad) have been excluded by definition in Committee Print No. 5. However, the application of the bill to a number of other files and information systems could seriously impair this Agency's mission.

Although section 203 provides limited exemptions for national defense or foreign policy reasons, certain sensitive intelligence sources and methods information arguably could not be exempted for these reasons even though its release would be damaging to the U.S. intelligence collection effort and the national interest and in conflict with the provisions of the National Security Act of 1947.

There are a number of other provisions in the bill which I believe could impair my capability to protect Intelligence Sources and Methods from unauthorized disclosure: (a) the Privacy Protection Commission, established under the bill, is granted absolute authority to investigate alleged violations; to conduct a study of standards and procedures to protect personal information; and to conduct hearings, take testimony, and subpoena witnesses and records as it deems necessary; (b) sections 104 and 105 require an agency to furnish any data, reports, or other information that the Commission deems necessary to carry out its functions; and (c) subsection 201(c)(3) requires the publication of specific data regarding files of personalities, including employees, and information systems maintained by the Agency.

Finally, section 304 grants jurisdiction to the district courts of the United States to hear civil actions brought under the Act and provides for an *in camera* examination and determination by the court of information for which an exemption is claimed under section 203. The Federal agency has the burden of establishing that the information is properly classified and that it is excludable under the Act. Perhaps I can best convey my view regarding this provision by quoting from a

20 August 1974 letter from President Ford to the Chairmen of the Conference Committee considering amendments to the Freedom of Information Act (H.R. 12471). Those amendments presently include a nearly identical judicial review provision:

"There are provisions . . . which would place the burden of proof upon an agency to satisfy a court that a document classified because it concerns military or intelligence (including intelligence sources and methods) secrets and diplomatic relations is, in fact, properly classified, following an *in camera* inspection of the document by the court. If the court is not convinced that the agency has adequately carried the burden, the document will be disclosed. I simply cannot accept a provision that would risk exposure of our military or intelligence secrets and diplomatic relations because of a judicially perceived failure to satisfy a burden of proof. My great respect for the courts does not prevent me from observing that they do not ordinarily have the background and expertise to gauge the ramifications that a release of a document may have upon our national security. The Constitution commits this responsibility and authority to the President. I understand that the purpose of this provision is to provide a means whereby improperly classified information may be detected and released to the public. This is an objective I can support as long as the means selected do not jeopardize our national security interests. I could accept a provision with an express presumption that the classification was proper and with *in camera* judicial review only after a review of the evidence did not indicate that the matter had been reasonably classified in the interests our national security. Following this review, the court could then disclose the document if it finds the classification to have been arbitrary, capricious, or without a reasonable basis." (10 Weekly Compilation of Presidential Documents, No. 34, Aug. 26, 1974).

In summary, it is my view that the protection of Intelligence Sources and Methods requires that practically all of our information on individuals and the details of our information systems must remain classified and not subject to public disclosure under S. 3418. As indicated in my earlier letter, it would be my preference that the Central Intelligence Agency be completely exempted from the bill. If this is not possible, it is requested that this Agency be granted a partial exemption (language enclosed).

The Office of Management and Budget advises there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,

W. E. Colby, *Director.*

Enclosure.

Insert as new subsection 203(d)

"(d) The provisions of subsection 103(a)(2), subsection 104(a), subsection 105(a)(1), section 106, subsection 201(c) [except subsections (2), (3)(B), (3)(D) and (3)(F)], subsections 201(d) and (f), and section 202 shall not apply to the Central Intelligence Agency. Nor shall any other provision of this Act be construed so as to impair or affect the authorities and responsibilities of the Director of Central

Intelligence under the National Security Act of 1947, as amended, or the Central Intelligence Agency Act of 1949, as amended."

[NOTE.—Other agency comments may be found in the hearing "Privacy," part 1.]

[From the Office of the White House Press Secretary, Feb. 23, 1974]

ADDRESS BY THE PRESIDENT ON THE AMERICAN RIGHT OF PRIVACY, LIVE ON NATIONWIDE RADIO, FROM THE WHITE HOUSE ON FEBRUARY 23, 1974

Over the years, historians and philosophers have continually debated about the roots of American greatness. There are almost as many theories as there have been scholars, but a single theme recurs again and again. It is the theme of individual dignity and individual rights—an ideal that permeates the Constitution's Bill of Rights and has been a fundamental part of American life since the founding of our Nation.

Generation after generation, we find America's best minds and greatest leaders emphasizing the need to protect the rights of the individual. In the Federalist Papers, James Madison said that the twin duties of enlightened government were "to secure the public good" and to secure "private rights." In our own time, President Eisenhower reaffirmed that ideal. He said, "The supreme belief of our society is in the dignity and freedom of the individual."

In James Madison's day, the American Revolution was fought to establish a new nation based on this principle. By the time Dwight Eisenhower was President, America had passed through a tragic Civil War and two bloody World Wars fought in defense of the same principle. But it is not on the battlefield alone that individual liberties are threatened and must be defended.

In peace as well as in war, social, economic, political and technological forces are constantly at work that can either help or hinder the individual American's quest for "life, liberty and the pursuit of happiness."

Many things are necessary to lead a full free life—good health, economic and educational opportunity, and a fair break in the marketplace, to name a few. But none of these is more important than the most basic of all individual rights, the right to privacy. A system that fails to respect its citizens' right to privacy, fails to respect the citizens themselves.

There are, of course, many facts which modern government must know in order to function. As a result, a vast store of personal data has been built up over the years. With the advent of the computer in the 1960's, this data gathering process has become a big business in the United States—over $20 billion a year—and the names of over 150 million Americans are now in computer banks scattered across the country.

At no time in the past has our Government known so much about so many of its individual citizens. This new knowledge brings with it an awesome potential for harm as well as good—and an equally awesome responsibility on those who have that knowledge.

Though well intentioned, Government bureaucracies seem to thrive on collecting additional information. That information is now stored in over 7,000 Government computers. Collection of new information will always be necessary. But there must also be reasonable limits on what is collected and how it is used.

The same process has been at work in the private sector where computers and modern data technology have placed vast quantities of personal information in the hands of bankers, employers, charitable organizations and credit agencies.

On the positive side, the availability of this information serves us all in many important ways.

Without computer technology, it would, for example, be extremely difficult to process and deliver 27 million Social Security checks every month, to send out veterans benefits, and to ensure that Medicare payments are properly made.

Law enforcement agencies would not and could not combat new and sophisticated criminal activities without the use of the latest technical developments in the data field, whether in helping to trace stolen goods, or in helping to track down and identify criminals.

In the private sector, the banking industry could not even start to cope with the vast volume of personal checks which are issued and cashed daily without using computer technology.

No modern industrial society can survive without computers and data processing—and especially a society with high living standards and even higher expectations such as ours.

Many of the good things in life that Americans take for granted would be impossible, or impossibly high-priced, without data retrieval systems and computer technology. But until the day comes when science finds a way of installing a conscience in every computer, we must develop human, personal safeguards, that prevent computers from becoming huge, mechanical, impersonal robots that deprive us of our essential liberties.

Here is the heart of the matter: What a person earns, what he owes, when he gives to his church or to his charity is his own personal business and should not be spread around without his consent. When personal information is given or obtained for one purpose such as a loan or credit at a store, it should not be secretly used by anyone for any other purpose.

To use James Madison's terms, in pursuing the overall public good, we must make sure that we also protect the individual's private rights.

There is ample evidence that at the present time this is not being adequately done. In too many cases unrestricted or improper use of personal information is being made.

In some instances, the information itself is inaccurate and has resulted in the withholding of credit or jobs from deserving individuals. In other cases, obsolete information has been used, such as arrest records which have not been updated to show that the charges made against an individual were subsequently dropped or the person found innocent. In many cases, the citizen is not even aware of what information is held on record, and if he wants to find out, he either has nowhere to turn or else he does not know where to turn.

Whether such information is provided and used by the Government or the private sector, the injury to the individual is the same. His right to privacy has been seriously damaged. So we find this happens sometimes beyond the point of repair. Frequently, the side effect is financial damage, but it sometimes goes further. Careers have been ruined, marriages have been wrecked, reputations built up over a lifetime have been destroyed by the misuse or abuse of data technology in both private and public hands.

It is clear, as one Government study has concluded, that "it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems." Fortunately more and more people are becoming aware of this growing threat.

The Fair Credit Reporting Act of 1970 which I signed into law took a major first step toward protecting the victims of erroneous or outdated information. It requires that an individual be notified when any adverse action, such as denial of credit, insurance or employment, is taken on the basis of a report from consumer-reporting agencies. It also provides citizens with a method of correcting these reports when they contain erroneous information.

Many public and private statistical organizations which collect personal data have shown an awareness of their own responsibility to prevent unfair disclosure and to eliminate inaccurate or obsolete information.

Earlier this month, Attorney General Saxbe proposed legislation to the Congress which would establish rules governing the collection and use of criminal justice information, and the Congress itself has conducted extensive hearings into the uses and the abuses of data banks, credit bureaus, and personal records.

All of this is action in the right direction, but we must go further and we must move quickly.

What was once a minor problem affecting only a small number of people has now become a national problem that could potentially affect every American with a charge account, a service or personnel record, a credit card, a Social Security number, a mortgage, or an appliance or automobile bought on time. In short, data banks affect nearly every man, woman and child in the United States today.

To meet a challenge of these dimensions, we need more than just another investigation and just another series of reports. We need action. That is why I am today establishing in the White House a top priority Domestic Council Committee on the Right of Privacy. This will not just be another research group. It will be a panel of some of the most able men and women in the Government, and it will be primed for high-level action.

It will be chaired by Vice President Ford, it will include the Attorney General and five other Cabinet members—the Secretaries of the Treasury, Defense, Commerce, Labor, and Health, Education, and Welfare—along with the Chairman of the Civil Service Commission, the Director of the Office of Management and Budget, the Director of the Office of Consumer Affairs, and the Director of the Office of Telecommunications Policy.

This is no ordinary group, and the task I have set for it is no ordinary task.

This Privacy Committee will build on the fine work that other groups have already carried out, and I will see to it that it is supported by the best talent available in determining the views of representatives from the legislative branch, the judicial branch and the private sector, including our colleges and universities.

I am asking the members to examine three key areas of concern: collection, storage and use of personal data. Specifically, the committee will examine:

How the Federal Government collects information on people and how that information is protected;

Procedures which would permit citizens to inspect and correct information held by public or private organizations;

Regulations of the use and dissemination of mailing lists;

And most importantly, ways that we can safeguard personal information against improper alteration or disclosure.

All of this will require extensive work by the Committee, but it is only the first half of the job.

Once the information and views of all parties concerned have been thoroughly aired, the Committee will be responsible for developing a comprehensive series of specific recommendations for action. I want that action to provide a personal shield for every American which he can use to protect his right to privacy.

I am directing this blue-ribbon panel, within four months, to begin providing a series of direct, enforceable measures—including regulations, executive actions, policy changes, legislation where necessary and voluntary restraints—all of which we can immediately begin to put into effect.

Advanced technology has created new opportunities for America as a Nation, but it has also created the possibility for new abuses of the individual American citizen. Adequate safeguards must always stand watch so that man remains the master—and never becomes the victim—of the computer.

In the first half of this century, Mr. Justice Brandeis called privacy the "right most valued by civilized men." In the last half of this century, we must also make it the right that is most protected.

Thank you and good afternoon.

[From the Congressional Record—Senate, Mar. 7, 1974]

ACTION FOR PRIVACY, SENATOR HART'S RESPONSE TO THE PRESIDENT

Mr. MUSKIE. Mr. President, last Saturday, our colleague and good friend, the senior Senator from Michigan (Mr. Hart) made a national radio broadcast giving the response of the congressional majority to the President's message on privacy legislation. Senator Hart not only exposed the inadequacy of the administration's proposals; he also set out a detailed program of effective action to end government spying on citizens and to control access to criminal records in government files. As he pointed out, the President can prove the sincerity of his concern for privacy by taking five different but related executive

actions, without waiting for legislative definition. Speaking for the Congress, he promised to work with the President to turn administration rhetoric into reality and said:

We look forward to a time when the tragedy of Watergate, and all it has come to represent, will also mark a decisive turning point in the preservation of our civil liberties.

Mr. President, Senator Hart's speech forthrightly defines our concerns over official invasions of privacy. I ask unanimous consent that it be printed in full in the Record for the benefit of all who seek to understand the realities of this vital issue.

There being no objection, the speech was ordered to be printed in the Record, as follows:

CONGRESSIONAL RESPONSE TO PRESIDENT NIXON'S MESSAGE ON PRIVACY

In his State of the Union Address, President Nixon promised to "make an historic beginning on the task of defending and protecting the right of personal privacy for every American."

That promise, subsequently outlined in the President's February 23rd radio address, turned out to be principally the naming of a new committee rather than a broad program of action.

The President's only specific proposal dealt with the one small part of the problem—the serious threat to personal privacy created by widespread use of data banks or computers. And even that was a halfway measure.

Despite all the disturbing revelations of Watergate, the President made no promise to instruct his administration to live up to the guarantees of personal privacy contained in the Constitution, nor did he give his support to several bills dealing with this which are already before Congress.

The fact is that Mr. Nixon is almost 200 years late in proclaiming a historic beginning in protecting personal privacy for every American. That foundation was laid in the Bill of Rights of the Constitution. The Founding Fathers, having led a revolution against the dictates of a king, knew that the cornerstone to liberty was strict prohibitions against government intrusion in the personal lives of its citizens.

The First Amendment to the Constitution guarantees citizens the right to speak or remain silent about their political beliefs, whether or not those beliefs agree or disagree with the government.

That means the federal government has no right to spy on political opponents, but the Nixon administration did just that.

The Fourth Amendment guarantees the right of people to be secure from unauthorized searches of their person, their house and their papers, but some either involved with President Nixon's election campaign or associated with his White House staff broke into at least two buildings seeking information.

When government officials use Army personnel to spy on peaceful political meetings, as the present Administration did, your privacy is threatened. When government officials send burglars to break into the offices of doctors for confidential files as this administration did with its Plumbers squad, your privacy is threatened.

When government officials use the confidential files of the Internal Revenue Service to harass persons on a White House enemies list, as this administration did, your privacy is threatened.

When government officials eavesdrop on private conversations of political opponents, as this administration did, your privacy is threatened.

Many of these actions by our government have been defended on grounds of "national security," but we have come to understand that there is a wide range of constitutional abuses a determined political operative can seek to have excused under that mantle. And, indeed, the American people realize that.

A recent poll, for example, showed that 75 percent of those interviewed considered "wiretapping and spying under the excuse of 'national security' as a serious threat to people's privacy."

As the public learned about government spying and wiretapping, it became fearful. Many have come to believe that their phones are tapped, their homes

or offices bugged, their mail opened, and their tax returns made available to officials who seek to punish them for political dissent.

This concern was underscored for me by a constituent who wrote not long ago. He (or possibly she) said he could not sign his name in a letter to his Senator anymore. He feared his letter might be intercepted and his name might go on a White House "enemies list".

While these fears may be exaggerated, they no longer can be dismissed as groundless paranoia. And they demonstrate the very real chilling effect on the exercise of First Amendment rights which the actions of the Administration have had.

No one denies that modern government needs certain kinds of information about its citizens to administer programs fairly and effectively. We must balance the right to be left alone against the needs of society. But we must always be guided by the need to keep government's ability to use information about private lives to the absolute minimum.

In his discussion of data banks, President Nixon did point to some very real threats to personal privacy. Federal agencies alone have files on every aspect of many of our lives—medical records, army records, school records, business records, to name a few. Consolidation of data could provide a tremendous amount of information for an unscrupulous official to use against us because of our views, our friends, or the way we live.

The pace of modern technology and data collection is a stiff challenge to maintaining privacy. However, and perhaps understandably in light of Watergate, the President chose to paint the primary threat as one of technology.

We have learned to our regret that, with or without sophisticated technology, unprincipled men can find ways to invade our privacy. A crowbar, after all, is a rather simple machine used to jimmy a door.

So if the President is serious about joining Congress in efforts to control government invasion of privacy, let me suggest a program of action he can take now.

Perhaps the most pressing need is to put an end to domestic political surveillance and intelligence gathering by government agencies. The President could begin that effort by supporting a Senate bill to prohibit military personnel from spying on American citizens.

The President should order everyone in his Administration to refrain from political spying of any kind. There is absolutely no justification, legal or otherwise, for government to collect intelligence on its political opponents for the purpose of or with the effect of stifling their opposition.

The President should immediately order that no wiretapping, bugging or breaking and entering, be carried out without authority of an independent court order.

He should state without equivocation that the label of "national security" will not be used again to hide or excuse illegal acts. And then he should join Congress in preparing legislation to make those executive orders into law.

The President should respond to continuing reports that telephone records, bank records and other private business records are being obtained by the government secretly with no legal safeguards—without the protection of a court warrant, or the opportunity for the person involved to raise legal objections to protect his rights. The President, by executive order, could and should end that practice and require any federal agency to obtain a subpoena for such information.

For several years, the Administration has opposed a Senate-passed bill to prohibit government employees from being asked about their religious beliefs, their politics and their social lives. The President should support this measure. Such a law would set an example for employers in the private sector to follow and free our civil servants from implied threats when that kind of information is sought.

And finally, the Administration should support stiffer controls on dissemination and use of criminal justice records than those contained in its current proposal.

These records include arrests as well as convictions. They are sold or given to credit bureaus, banks, insurance companies, employers, and schools. Too many people have been denied advanced schooling, a loan or a job because of inaccurate records or because an arrest record fails to include the fact that charges were later dropped or the person was acquitted.

And too many people never find out that such records exist and cause their difficulties.

The answer is a law to prevent private access to all arrest records and require officials to open these records to inspection and correction by those involved. And any criminal justice agency participating in the nationwide criminal information network should be required to update their records.

I have outlined a program of action I would hope the President would adopt. In doing so, he would turn his back on what I believe to be unprecedented efforts in this Administration to undermine the right to privacy and he would live up to the rhetoric of his message on that right.

We in Congress are fully prepared to work with him toward that end. We look forward to a time when the tragedy of Watergate, and all it has come to represent, will also mark a decisive turning point in the preservation of our civil liberties.

As it is with many rights necessary to keep a country free, we do not always understand the importance of the guarantee to privacy until it has been threatened.

But defend it we must or else cease to be a land which would be free.

Justice Louis Brandeis once wrote that our Founding Fathers:

"Sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be left alone—the most comprehensive right and the right most valued by civilized man."

We must not surrender that most valued right.

Thank you.

CHAPTER II

Developments Since Enactment

63-619 O - 76 - 65

Guidelines For Implementing
Section 552a of Title 5
of the United States Code

(Section 3 of the Privacy Act of 1974, Public Law 93-579).

PRIVACY ACT GUIDELINES - July 1, 1975

TABLE OF CONTENTS

Subsection

(a) DEFINITIONS

(1) Agency
(2) Individual
(3) Maintain
(4) Record
(5) System of Records
(6) Statistical Record
(7) Routine Use

(b) CONDITIONS OF DISCLOSURE

(1) Disclosure within the Agency
(2) Disclosure to the Public
(3) Disclosure for a "Routine Use"
(4) Disclosure to the Bureau of the Census
(5) Disclosure for Statistical Research and Reporting
(6) Disclosure to the National Archives
(7) Disclosure for Law Enforcement Purposes
(8) Disclosure under Emergency Circumstances
(9) Disclosure to the Congress
(10) Disclosure to the General Accounting Office
(11) Disclosure Pursuant to Court Order

(c) ACCOUNTING OF CERTAIN DISCLOSURES

(1) When Accounting is Required
(2) Retaining the Accounting of Disclosures
(3) Making the Accounting of Disclosures Available to the Individual
(4) Informing Prior Recipients of Corrected or Disputed Records

(d) ACCESS TO RECORDS

(1) Individual Access to Records
(2) Requests for Amending Records
(A) Acknowledgement of Requests to Amend Records
(B) Actions Required on Requests to Amend Records
(3) Requesting a Review of the Agency's Refusal to Amend a Record
(4) Disclosure of Disputed Information
(5) Access to Information Compiled in Anticipation of Civil Action

(e) AGENCY REQUIREMENTS

(1) Restrictions on Collecting Information about Individuals
(2) Information is to be Collected Directly from the Individual
(3) Informing Individuals from Whom Information is Requested
(4) Publication of the Annual Notice of Systems of Records
  (A) Describing the Name and Location of the System in the Public Notice
  (B) Describing Categories of Individuals in the Public Notice
  (C) Describing Categories of Records in the Public Notice
  (D) Describing Routine Uses in the Public Notice
  (E) Describing Records Management Policies and Practices in the Public Notice
  (F) Identifying Official(s) Responsible for the System in the Public Notice
  (G) Describing Procedures for Determining if a System contains a Record on an Individual in the Public Notice
  (H) Describing Procedures for Gaining Access in the Public Notice
  (I) Describing Categories of Information Sources in the Public Notice
(5) Standards of Accuracy
(6) Validating Records before Disclosure
(7) Records on Religious or Political Activities
(8) Notification for Disclosures Under Compulsory Legal Process
(9) Rules of Conduct for Agency Personnel
(10) Administrative, Technical and Physical Safeguards
(11) Notice for New/Revised Routine Uses

(f) AGENCY RULES

(1) Rules for Determining if an Individual is the Subject of a Record
(2) Rules for Handling Requests for Access
(3) Rules for Granting Access to Records
(4) Rules for Amending Records
(5) Rules Regarding Fees
Annual Publication of Notices and Rules

(g) CIVIL REMEDIES

(1) Grounds for Action
  (A) Refusal to Amend a Record
  (B) Denial of Access to a Record
  (C) Failure to Maintain a Record Accurately
  (D) Other Failures to Comply with the Act
(2) Basis for Judicial Review and Remedies for Refusal to Amend a Record

(3) Basis for Judicial Review and Remedies for Denial of Access
(4) Basis for Judicial Review and Remedies for Adverse Determination and Other Failures to Comply
(5) Jurisdiction and Time Limits

(h) RIGHTS OF LEGAL GUARDIANS

(i) CRIMINAL PENALTIES

(1) Criminal Penalties for Unauthorized Disclosure
(2) Criminal Penalties for Failure to Publish a Public Notice
(3) Criminal Penalties for Obtaining Records Under False Pretenses

(j) & (k) EXEMPTIONS

(j) GENERAL EXEMPTIONS APPLICABILITY AND NOTICE REQUIREMENTS

(1) General Exemption for the Central Intelligence Agency
(2) General Exemption for Criminal Law Enforcement Records

(k) SPECIFIC EXEMPTIONS APPLICABILITY AND NOTICE REQUIREMENTS

(1) Exemption for Classified Material
(2) Exemption for Investigatory Material Compiled for Law Enforcement Purposes
(3) Exemption for Records Maintained to Provide Protective Services
(4) Exemption for Statistical Records
(5) Exemption for Investigatory Material Compiled for Determining Suitability for Federal Employment or Military Service
(6) Exemption for Testing or Examination Material
(7) Exemption for Material used to Evaluate Potential for Promotion in the Armed Services

(l) ARCHIVAL RECORDS

(1) Records Stored in GSA Records Centers
(2) Records Archived Prior to September 27, 1975
(3) Records Archived on or after September 27, 1975

(m) GOVERNMENT CONTRACTORS

(n) MAILING LISTS

(o) REPORT ON NEW SYSTEMS

(p) ANNUAL REPORT

(q) EFFECT OF OTHER LAWS

Subsection (a)

DEFINITIONS

Subsection (a) "For purposes of this section ---"

AGENCY

Subsection (a)(1) "The term 'agency' means agency as defined in section 552(e) of this title;"

The definition of "agency" is the same as that used in the Administrative Procedures Act as modified by the recently enacted Freedom of Information Act amendments (P.L. 93-502): "'agency' means each authority of the Government of the United States, whether or not it is within or subject to review by another agency... "(5.U.S.C. 551(1)). "[T]he term agency...includes any executive department, military department, Government corporation, Government controlled corporation or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." (5 U.S.C 552(e) as added by P.L. 93-502)

Two aspects of this definition require further explanation

- the scope of the term; i.e., what entities are covered, how has the definition of agency been broadened to encompass additional organizations as a result of the FOIA amendments?
- whether or not entities within an agency are to be considered agencies. This is particularly significant in applying subsection (b)(1), in determining what constitutes an inter agency transfer.

The first question - the scope of the definition - is covered in the House report on the FOIA amendments quoted below, as modified by the conference report language set out thereafter:

"For the purposes of this section, the definition of 'agency' has been expanded to include those entities which may not be considered agencies under section 551(1) of title 5, U.S. Code,

but which perform governmental functions and control information of interest to the public. The bill expands the definition of 'agency' for purposes of section 552, [and 552a] title 5, United States Code. Its effect is to insure inclusion under the Act of Government corporations, Government controlled corporations, or other establishments within the executive branch, such as the U.S. Postal Service.

"The term 'establishment in the Executive Office of the President,' as used in this amendment means such functional entities as the Office of Telecommunications Policy, the Office of Management and Budget, the Council of Economic Advisers, the National Security Council, the Federal Property Council, and other similar establishments which have been or may in the future be created by Congress through statute or by Executive order.

"The term 'Government corporation,' as used in this subsection, would include a corporation that is a wholly Government-owned enterprise, established by Congress through statute, such as the St. Lawrence Seaway Development Corporation, the Federal Crop Insurance Corporation (FCIC), the Tennessee Valley Authority (TVA), and the Inter-American Foundation.

"The term 'Government controlled Corporation,' as used in this subsection, would include a corporation which is not owned by the Federal Government ..." (House Document 93-876, pp.8-9, Report on the Freedom of Information Act amendments, H.R. 12741)

"The conferees state that they intend to include within the definition of 'agency' those entities encompassed by 5 U.S.C. 551 and other entities including the United States Postal Service, the Postal Rate Commission, and government corporations or government-controlled corporations now in existence or which may be created in the future. They do not intend to include corporations which receive appropriated funds but are neither chartered by the Federal Government nor controlled by it, such as the Corporation for Public Broadcasting. Expansion of the definition of 'agency' in this subsection is intended to broaden applicability of the Freedom of Information Act but it is not intended that the term 'agency' be applied to subdivisions, offices or units within an agency.

"With respect to the meaning of the term 'Executive Office of the President' the conferees intend the result reached in Soucie v. David , 448 F.2d. 1067 (C.A.D.C. 1971). The term is not to be interpreted as including the President's immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President." (House Report 93-1380, p 14-15)

Whether or not an agency can exist within an agency is a somewhat more complex issue. This is addressed, in part, in the above quotation from the conference report language in the statement ".. but it is not intended that the term 'agency' be applied to subdivisions, offices,

or units within an agency." The issue was also addressed in debate on HR 16373 on the House floor in a statement by Congressman Moorhead - "... 'agency' is given the meaning which it carries elsewhere in the Freedom of Information Act, 5 United States Code, section 551(1), as amended by H.R. 12471 of this Congress, section 552(e), on which Congress has acted to override the veto. The present bill is intended to give 'agency' its broadest statutory meaning. This will permit employees and officers of the agency which maintains the records to have access to such records if they have a need for them in the performance of their duties. For example, within the Justice Department--which is an agency under the bill--transfer between divisions of the Department, the U.S. Attorney's offices, the Parole Board, and the Federal Bureau of Investigation would be on a need-for-the-record basis. Transfer outside the Justice Department to other agencies would be more specifically regulated. Thus, transfer of information between the FBI and the Criminal Division of the Justice Department for official purposes would not require additional showing or authority, in contrast to transfer of such information from the FBI to the Labor Department." (Congressional Record November 21, 1974, p. H10962)

In addressing this question the Justice Department has advised that

> "... it is our firm view that the 1974 [POIA] Amendments require no change in the original Act, that it is for the over-unit -- the Department or other higher-level 'agency' -- to determine which of its substantially independent components will function independently for Freedom of Information Act purposes. Moreover, as the Attorney General noted in that portion of his Memorandum dealing with the subject, 'it is sometimes permissible to make the determination differently for purposes of various provisions of the Act -- for example, to publish and maintain an index at the overunit level while letting the appropriate subunits handle requests for their own records.' (Attorney General's Memorandum on the 1974 Amendments to the Freedom of Information Act, February, 1975, p. 26). In our view, this practice of giving variable content to the meaning of the word 'agency' for various purposes can be applied to the Privacy Act as well as the Freedom of Information Act. For example, it may be desirable and in furtherance of the purposes of the Act to treat the various components of a Department as separate 'agencies' for purposes of entertaining applications for access and ruling upon appeals from denials, while treating the Department as the 'agency' for purposes of those provisions limiting intragovernmental exchange of records. (Of course, dissemination among components of the Department must still be only on a 'need-to-know' basis. 5 U.S.C. 552a(b)(1).) Needless to say, this practice must not be employed invidiously, so as to frustrate rather than to further the purposes of the Act; and there should be a consistency between the practice under the Privacy Act and the practice for comparable purposes under the Freedom of Information Act. For this reason it seems to us doubtful (though not entirely impossible) that a Department or other over-unit which has

> treated its components as separate agencies for all purposes under the Freedom of Information Act could successfully maintain that all of its components can be considered a single 'agency' under the Privacy Act, simply to facilitate the exchange of records "(Letter from Assistant Attorney General, Office of Legal Counsel, dated April 14, 1975)

In addition to the matter of determining when a component of an agency is to be considered an agency itself and when the entire agency is to be treated as a single entity, the issue arises as to whether an entity or individual serving more than one agency may be considered an "employee" of each agency he serves, for certain purposes. While this is not specifically addressed in the Act, it is reasonable to assume that members of temporary task forces, composed of personnel of several agencies, should usually be considered employees of the lead agency and of their own agency for purposes of access to information. Similarly, members of permanent "strike forces" and personnel cross-designated to serve the functions of two or more agencies should usually be treated as employees of both the lead agency and their own employing agency, e.g., employees or State or local officials assigned to organized crime, and customs officers cross designated to perform each others functions.

INDIVIDUAL

> Subsection (a)(2) "The term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence;"

This definition is intended to "distinguish between the rights which are given to the citizen as an individual under this Act and the rights of proprietorships, businesses, and corporations which are not intended to be covered by this Act. This distinction was to insure that the bill leaves untouched the Federal Government's information activities for such purposes as economic regulations. This definition was also included to exempt from the coverage of the bill intelligence files and data banks devoted solely to foreign nationals or maintained by the State Department, the Central Intelligence Agency and other agencies for the purpose of dealing with nonresident aliens and people in other countries." (Senate Report 93-1183, p. 79).

The language cited above suggests that a distinction can be made between individuals acting in a personal capacity and individuals acting in an entrepreneurial capacity (e.g., as sole proprietors) and that this definition (and, therefore, the Act) was intended to embrace only the former. This distinction is, of course crucial to the application of the Act since the Act, for the most part, addresses

"records" which are defined as "... information about individuals" (subsection (a)(4)). Agencies should examine the content of the records in question to determine whether the information being maintained is, in fact, personal in nature. A secondary criterion in deciding whether the subject of an agency file is, for purposes of the Act, an individual, is the manner in which the information is used; i.e., is the subject dealt with in a personal or entrepreneurial role.

Files relating solely to nonresident aliens are not covered by any portion of the Act. Where a system of records covers both citizens and nonresident aliens, only that portion which relates to citizens or resident aliens is subject to the Act but agencies are encouraged to treat such systems as if they were, in their entirety, subject to the Act.

The Act and the legislative history are silent as to whether a decedent may be considered to be an individual and whether anyone may authorize the rights of the decedent to records pertaining to him maintained by Federal agencies. It would appear that the thrust of the Act was to provide certain statutory rights to living as opposed to deceased individuals. But for the provision enabling parents to act on behalf of minors and guardians to act on behalf of those deemed to be incompetent, the rights of an individual provided by the Privacy Act could not have been utilized in their behalf by those interested. The failure of the Privacy Act to so provide for decedents and the overall thrust of the Act - that individuals be given the opportunity to judge for themselves how, and the extent to which, certain information about them maintained by Federal agencies is used, and the implicit personal judgement involved in this thrust - indicates that the Act did not contemplate permitting relatives and other interested parties to exercise rights granted by the Privacy Act to individuals after the demise of those individuals. These same records, however, may pertain as well to those living persons who might otherwise seek to exercise the decedent's right with regard to that information and thereby be covered by the Privacy Act. Furthermore, access to a decedent's records may be had in various judicial forums as a part of, or ancillary to, other proceedings.

MAINTAIN

> Subsection (a)(3) "The term 'maintain' includes maintain, collect, use, or disseminate;"

The term 'maintain' is used in two ways in the Privacy Act.

First, it is used to connote the various record keeping functions to which the requirements of the Act apply; i.e., maintaining, collecting, using, or disseminating. Thus, wherever the word "maintain" appears with reference to a record, one should understand

it to mean collect, use, or disseminate or any combination of any of these record-keeping functions.

Second, it is used to connote control over and hence responsibility and accountability for systems of records. This is extremely important given the civil and criminal sanctions in subsections (g) and (i) for failure to comply with certain provisions. The applicability of certain provisions, including the exemptions in subsections (j) and (k), can be determined by an agency's ability to demonstrate that it has effective control over a system of records. See, for example, subsections (b)(1), (d), (e)(1), (e)(9), (g), and (i) wherein the term "maintain" clearly means having effective control over a system of records. To have effective control of a system of records does not necessarily mean to have physical control of the system. When records are disclosed to Agency B from a system of records maintained by Agency A, they are then considered to be maintained by Agency B (as well as Agency A) and are subject to all of the provisions of the Act in the same manner as though Agency B had originally compiled them. If one agency turns over a record from its system of records to a second agency and that record is placed in a separate system of records maintained by the second agency, then the record becomes part of the system of records maintained by the second agency and all of the published material as to the second agency's system of records would apply to the record moved into its system.

The requirements of subsection (m) must also be carefully considered in determining which systems are to be considered as "maintained," i.e., controlled by an agency within the terms of the Act. Subsection (m) stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandates "by or on behalf of the agency...to accomplish an agency function" are subject to the provisions of Section 3 of the Act. The intent of this provision is to make it clear that the systems "maintained" by an agency are not limited to those operated by agency personnel on agency premises but include certain systems operated pursuant to the terms of a contract to which the agency is a party. The qualifying phrase "to accomplish an agency function" limits the applicability of subsection (m) to those systems directly related to the performance of Federal agency functions by excluding from its coverage systems which are financed, in whole or part, with Federal funds, but which are managed by state or local governments for the benefit of State or local governments.

RECORD

> Subsection (a)(4) "The term 'record' means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;"

The term "record", as defined for purposes of the Act, means a tangible or documentary record (as opposed to a record contained in someone's memory) and has a broader meaning than the term commonly has when used in connection with record- keeping systems. (It may also differ from the usual definition of a computer record.) An understanding of the term "record", as it is used in the Act, is essential in interpreting the meaning of many of the Act's requirements.

A "record"

- means any item of information about an individual that includes an individual identifier;
- includes any grouping of such items of information (it should not be confused with the use of the term record in the conventional sense or as used in the automatic data processing (ADP) community);
- does not distinguish between data and information; both are within the scope of the definition; and
- includes individual identifiers in any form including, but not limited to, finger prints, voice prints and photographs.

The phrase "identifying particular" suggests any element of data (name, number) or other descriptor (finger print, voice print, photographs) which can be used to identify an individual. Identifying particulars are not always unique (i.e., many individuals share the same name) but when they are not unique (e.g., name) they are individually assigned - as distinguished from generic characteristics.

The term "record" was defined "to assure the intent that a record can include as little as one descriptive item about an individual." (Congressional Record , p. S21818, December 17, 1974 and p. H12246, December 18, 1974). This definition "includes the record of present registration, or membership in an organization or activity, or admission to an institution." (Senate Report 93-1183, p. 79). (While this language was written with reference to the definition of the term "personal information" in the Senate bill, it would appear to be equally applicable to the term "record" as used in the Act.)

A record, by this definition, can be part of another record. Therefore prohibitions on the disclosure of a record, for example, apply not only to the entire record in the conventional sense (such as a record in a computer system), but also to any item or grouping of items from a record provided that such grouping includes an individual identifier.

SYSTEM OF RECORDS

> Subsection (a) (5) "The term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;"

The definition of "system of records" limits the applicability of some of the provisions of the Act to "records" which are maintained by an agency, retrieved by individual identifier (i.e., there is an indexing or retrievel capability using identifying particulars, as discussed above, built into the system), and the agency does, in fact, retrieve records about individuals by reference to some personal identifier.

A system of records for purposes of the Act must meet all of the following three criteria:

- It must consist of records. See discussions of "record", (a) (4), above.
- It must be "under the control of" an agency.
- It must consist of records retrieved by reference to an individual name or some other personal identifier.

The phrase "...under the control of any agency..." was intended to accomplish two separate purposes: (1) to determine possession and establish accountability; and (2) to separate agency records from records which are maintained personally by employees of an agency but which are not agency records.

As previously noted, the definition of "maintain" was broadened to encompass all systems used by Federal agencies. The phrase "...under the control of any agency..." in the definition of "system of records" was not intended to eliminate from the coverage of the Act any of those systems (which would largely negate the definition of "maintain"), but rather was intended to assign responsibility to a particular agency to discharge the obligations established by the Privacy Act. An agency is responsible for those systems which are "...under the control of" that agency. The concept of possession implicit in this phrase is also apparent in the language which begins most of the operative subsections of the Act. For example, the concept is evident although tacit in subsection (b); express in subsection (c) "under its control...", "...that maintains a system of records..." in subsections (d), (e) and (f); "agency records" in subsection (i), and "...any system of records within the agency" in subsection (j) and (k).

The intent was, despite the different wording for each subsection, not to have each of the subsections apply to a different roster of systems of records, but to express, in terms of possession, for which systems of records an agency was responsible.

The second purpose of the phrase was to distinguish "agency records" from those records which, although in the physical possession of agency employees and used by them in performing official functions, were not considered "agency records." Uncirculated personal notes, papers and records which are retained or discarded at the author's discretion and over which the agency exercises no control or dominion (e.g., personal telephone lists) are not considered to be agency records within the meaning of the Privacy Act. This distinction is embodied, in part, in the phrase "under the control of" an agency as well as in the defintion of 'record' (5 USC 552 (a)(4)).

AN AGENCY SHALL NOT CLASSIFY RECORDS, WHICH ARE CONTROLLED AND MAINTAINED BY IT, AS NON-AGENCY RECORDS, IN ORDER TO AVOID PUBLISHING NOTICES OF THEIR EXISTENCE, PREVENT ACCESS BY THE INDIVIDUALS TO WHOM THEY PERTAIN, OR OTHERWISE EVADE THE REQUIREMENTS OF THE ACT.

The "are retrieved by" criterion implies that the grouping of records under the control of an agency is accessed by the agency by use of a personal identifier; not merely that a capability or potential for retrieval exists. For example, an agency record-keeping system on firms it regulates may contain "records" (i.e., personal information) about officers of the firm incident to evaluating the firm's performance. Even though these are clearly "records" "under the control of" an agency, they would not be considered part of a system as defined by the Act unless the agency accessed them by reference to a personal identifier (name, etc.). That is, if these hypothetical "records" are never retrieved except by reference to company identifier or some other nonpersonal indexing scheme (e.g., type of firm) they are not a part of a system of records. Agencies will necessarily have to make determinations on a system-by-system basis.

Considerable latitude is left to the agency in defining the scope or grouping of records which constitute a system. Conceivably all the "records" for a particular program can be considered a single system or the agency may consider it appropriate to segment a system by function or geographic unit and treat each segment as a "system". The implications of these decisions and some limitations on them are discussed in connection with subsection (e) (4), publication of the annual notice. Briefly, the two considerations which the agency should take into account in its decisions are

- its ability to comply with the requirements of the Act and facilitate the exercise of the rights of individuals; and
- the cost and convenience to the agency, but only to the extent consistent with the first consideration.

STATISTICAL RECORD

Subsection (a)(6) "The term 'statistical record' means a record in a system of records maintained for statistical research or

reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;"

A "statistical record", for purposes of this Act, is a record in a system of records that is not used by anyone in making any determination about an individual. This means that, for a record to qualify as a "statistical record", it must be held in a system which is separated from systems (some perhaps containing the same information) which contain records that are used in any manner in making decisions about the rights, benefits, or entitlements of an identifiable individual. The term "identifiable individual" is used to distinguish determinations about specific individuals from determinations about aggregates of individuals as, for example, census data are used to apportion funds on the basis of population.

By this definition, it appears that some so-called "research records" which are only used for analytic purposes qualify as "statistical records" under the Act if they are not used in making determinations. A "determination" is defined as "any decision affecting the individual which is in whole or in part based on information contained in the record and which is made by any person or any agency." (House Report 93-1416, p.15.)

Most of the records of the Bureau of the Census are considered to be "statistical records" even though, pursuant to section 8 of title 13, United States Code, the Census Bureau is authorized to "furnish transcripts of census records for genealogical and other proper purposes and to make special statistical surveys from census data for a fee upon request." (House report 93-1416, p. 12)

In applying this definition, it might be helpful to distinguish three types of collections or groupings of information about individuals: (1) statistical compilations which, because they cannot be identified with individuals, are not subject to the Act at all; (2) "records" maintained solely for the purpose of compiling statistics -which are the types of records covered by (a)(6); and (3) "records" on individuals which are used both to compile statistics and also for other purposes, e.g. a criminal history record used both to compile individual statistics and to assist a judge in making a sentencing decision about the individual to whom the record pertains, which is not a "statistical record."

The term "statistical record" is used in subsection (k) (4), specific exemptions.

ROUTINE USE

63-619 O - 76 - 66

Subsection (a)(7) "The term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."

One of the primary objectives of the Act is to restrict the use of information to the purposes for which it was collected. The term "routine use" was introduced to recognize the practical limitations of restricting use of information to explicit and expressed purposes for which it was collected. It recognizes that there are corollary purposes "compatible with the purpose for which [the information] was collected" that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public. Routine uses include "transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information." (Congressional Record p. S21816, December 17, 1974 and p. H12244, December 18, 1974)

Additional guidance on the conceptual basis for "routine uses" is found in the statement of Congressman Moorhead on the House floor:

"It would be an impossible legislative task to attempt to set forth all of the appropriate uses of Federal records about an identifiable individual. It is not the purpose of the bill to restrict such ordinary uses of the information. Rather than attempting to specify each proper use of such records, the bill gives each Federal agency the authority to set forth the 'routine' purposes for which the records are to be used under the guidance contained in the committee's report.

"In this sense 'routine use' does not encompass merely the common and ordinary uses to which records are put, but also includes all of the proper and necessary uses even if any such use occurs infrequently. For example, individual income tax return records are routinely used for auditing the determination of the amount of tax due and for assistance in collection of such tax by civil proceedings. They are less often used, however, for referral to the Justice Department for possible criminal prosecution in the event of possible fraud or tax evasion, though no one would argue that such referral is improper; thus the 'routine' use of such records and subsection (b)(3) might be appropriately construed to permit the Internal Revenue Service to list in its regulations such a referral as a 'routine use.'

"Again, if a Federal agency such as the Housing and Urban Development Department or the Small Business Administration were to discover a possible fraudulent scheme in one of its programs it could 'routinely', as it does today, refer the relevant

records to the Department of Justice, or its investigatory arm, the FBI.

> "Mr Chairman, the bill obviously is not intended to prohibit such necessary exchanges of information, providing its rulemaking procedures are followed. It is intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes. To this end it would be sufficient if an agency publishes as a 'routine use' of its information gathered in any program that an apparent violation of the law will be referred to the appropriate law enforcement authorities for investigation and possible criminal prosecution, civil court action, or regulatory order." (Congressional Record, November 21, 1974, p.H10962)

In discussing the final language of the Act, Senator Ervin and Congressman Moorhead, in similar statements said that "[t]he compromise definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." (Congressional Record, December 17, 1974, p S21816 and December 18, 1974, p H12244) This implies, at least, that a "routine use" must be not only compatible with, but related to, the purpose for which the record is maintained; e.g., development of a sampling frame for an evaluation study or other statistical purposes.

There are certain "routine uses" which are applicable to a substantial number of systems of records but which are only permissible if properly established by each agency:

- disclosures to a law enforcement agency when criminal misconduct is suspected in connection with the administration of a program; e.g., apparently falsified statements on a grant application or suspected fraud on a contract.

- disclosures to an investigative agency in the process of requesting that a background or suitability investigation be conducted on individuals being cleared for access to classified information, employment on contracts, or appointment to a position within the agency.

The Act further limits the extent to which disclosures can be made as "routine uses" by requiring an agency to establish the "routine uses" of information in each system of records which it maintains by publishing a declaration of intent in the Federal Register, thereby permitting public review and comment (subsection (e)(11)).

Subsection (b)
CONDITIONS OF DISCLOSURE

Subsection (b) "No agency shall dislose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--"

This subsection provides that an agency may not disclose any record contained in system of records, as defined in subsection (a)(5) above, to any person or to any other agency unless the agency which maintains the record is requested to do so by the individual to whom the record pertains or the agency has obtained the written consent of the individual or the disclosure would fall within one or more of the categories enumerated in subsections (b)(1) through (11), below. The phrase "by any means of communication" means any type of disclosure (e.g., oral disclosure, written disclosure,electronic or mechanical tranfers between computers of the contents of a record).

Disclosure, however, is permissive not mandatory . An agency is authorized to disclose a record for any purpose enumerated below when it deems that disclosure to be appropriate and consistent with the letter and intent of the Act and these guidelines.

NOTHING IN THE PRIVACY ACT SHOULD BE INTERPRETED TO AUTHORIZE OR COMPEL DISCLOSURES OF RECORDS, NOT OTHERWISE PERMITTED OR REQUIRED, TO ANYONE OTHER THAN THE INDIVIDUAL TO WHOM A RECORD PERTAINS PURSUANT TO A REQUEST BY THE INDIVIDUAL FOR ACCESS TO IT.

Agencies shall not automatically disclose a record to someone other than the individual to whom it pertains simply because such a disclosure is permitted by this subsection. Agencies shall continue to abide by other constraints on their authority to disclose information to a third party including, where appropriate, the likely effect upon the individual of making that disclosure. Except as prescribed in subsection (d)(1), (individual access to records) this Act does not require disclosure of a record to anyone other than the individual to whom the record pertains.

A disclosure may be either the transfer of a record or the granting of access to a record.

The fact that an individual is informed of the purposes for which information will be used when information is collected pursuant to subsection (e)(3) does not constitute consent.

There are two instances in which consent to disclose a record might be actively sought by an agency (i.e., without waiting for the individual to request that a disclosure be made).

- Disclosure would properly be a "routine use" (b)(3)) but disclosure is proposed to be made before the 30 day notice period; e.g., the agency is developing a sampling frame for an evaluation study or a statistical program directly related to the purpose for which the record was established.

- Disclosure is unrelated to the purpose for which the record is maintained but the individual may wish to elect to have his or her record disclosed; e.g., to have information on a Federal employment application referred to State agencies or to permit information on such an application to be checked against other Federal agency's records.

In either case, however, care must be exercised to assure that the language of the request is not coercive and that any consequences of refusing to consent are made clear. It is particularly important that the impression not be created that consent to disclose is a prerequisite to obtaining a benefit when it is not.

The consent provision of this subsection was not intended to permit a blanket or open-ended consent clause; i.e., one which would permit the agency to disclose a record without limit. At a minimum, the consent clause should state the general purposes for, or types of recipients, to which disclosure may be made.

A record in a system of records may be disclosed without either a request from or the written consent of the individual to whom the record pertains only if disclosure is authorized below.

DISCLOSURE WITHIN THE AGENCY

Subsection (b)(1) "To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;"

This provision is based on a "need to know" concept. See also definition of "agency," (a)(1). It is recognized that agency personnel require access to records to discharge their duties. In discussing the conditions of disclosure provision generally, the House Committee said that "it is not the Committee's intent to impede the orderly conduct of government or delay services performed in the interests of the individual. Under the conditional disclosure provisions of the bill, 'routine' transfers will be permitted without the necessity of prior written consent. A 'non-routine' transfer is generally one in which the personal information on an individual is used for a purpose other than originally intended." (House Report 93-1416, p. 12).

This discussion suggests that some constraints on the transfer of records within the agency were intended irrespective of the definition of agency. Minimally, the recipient officer or employee must have an official "need to know." The language would also seem to imply that the use should be generally related to the purpose for which the record is maintained.

Movement of records between personnel of different agencies may in some instances be viewed as intra-agency disclosures if that movement is in connection with an inter-agency support agreement. For example, the payroll records compiled by Agency A to support Agency B in a cross- service arrangement are, arguably, being maintained by Agency A as if it were an employee of Agency B. While such transfers would meet the criteria both for intra-agency disclosure and "routine use," they should be treated as intra-agency disclosures for purposes of the accounting requirements (e)(1). In this case, however, Agency B would remain responsible and liable for the maintenance of such records in conformance with the Act.

It should be noted that the conditions of disclosure language makes no specific provision for disclosures expressly required by law other than 5 U.S.C. 552. Such disclosures, which are in effect congressionally-mandated "routine uses," should still be established as "routine uses" pursuant to subsection (e)(11) and (e)(4)(D). This is not to suggest that a "routine use" must be specifically prescribed in law.

DISCLOSURE TO THE PUBLIC

Subsection (b)(2) "Required under section 552 of this title;"

Subsection (b)(2) is intended "to preserve the status quo as interpreted by the courts regarding the disclosure of personal information" to the public under the Freedom of Information Act (Congressional Record p. S21817, December 17, 1974 and p. H12244, December 18, 1974). It absolves the agency of any obligation to obtain the consent of an individual before disclosing a record about him or her to a member of the public to whom the agency is required to disclose such information under the Freedom of Information Act and permits an agency to withhold a record about an individual from a member of the public only to the extent that it is permitted to do so under the exemptions to the FOIA (5.U.S.C. 552 (b)). Given the use of the term "required", agencies may not voluntarily make public any record which they are not required to release (i.e., those that they are permitted to withhold) without the consent of the individual unless that disclosure is permitted under one of the other portions of this subsection.

Records which have traditionally been considered to be in the public domain and are required to be disclosed to the public, such as many of the final orders and opinions of quasi-judicial agencies, press releases, etc. may be released under this provision without waiting for a specific Freedom of Information Act request. For example, opinions of quasi-judicial agencies may be sent to counsel for the

parties and to legal reporting services, and press releases may be issued by agencies dealing with public record matters such as suits commenced or agency proceedings initiated. Records which the agency would elect to disclose to the public but which are not required to be disclosed (i.e., they are permitted to be withheld under the FOIA) may only be released to the public under the "routine use" provision (subsection (b)(3)). Note, however, that an agency may not rely on any provision of the Freedom of Information Act as a basis for refusing access to a record to the individual to whom it pertains, unless such refusal of access is authorized by an exemption within the Privacy Act. See subsections (d) (1) and (g) below.

DISCLOSURE FOR A "ROUTINE USE"

> Subsection (b)(3) "For a routine use as defined in subsection (a)(7) of this section and described under subsection (e) (4)(D) of this section;"

Records may be disclosed without the prior consent of the individual for a "routine use", as defined above, if that "routine use" has been established and described in the public notice about the system published pursuant to subsections (e)(4)(D), and (e)(11) below.

DISCLOSURE TO THE BUREAU OF THE CENSUS

> Subsection (b)(4) "To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;"

Agencies may disclose records to the Census Bureau in individually identifiable form for use by the Census Bureau pursuant to the provisions of Title 13. (Title 13 not only limits the uses which may be made of these records but also makes them immune from compulsory disclosure).

DISCLOSURE FOR STATISTICAL RESEARCH AND REPORTING

> Subsection (b)(5) "To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;"

Agencies may disclose records for statistical purposes under limited conditions. The use of the phrase "in a form that is not individually identifiable" means not only that the information disclosed or transferred must be stripped of individual identifiers but also that the identity of the individual can not reasonably be deduced by anyone from tabulations or other presentations of the information (i.e., the identity of the individual can not be determined or deduced by combining various statistical records or by reference to public records or other available sources of information.) See also the discussion of "statistical record" ((a) (6)), above.

Records, whether or not statistical records as defined in (a)(6), above, may be disclosed for statistical research or reporting purposes only after the agency which maintains the record has received and evaluated a written statement which:

- states the purpose for requesting the records; and
- certifies that they will only be used as statistical records.

Such written statements will be made part of the agency's accounting of disclosures under subsection (c)(1).

Fundamentally, agencies disclosing records under this provision are required to assure that information disclosed for use as a statistical research or reporting record cannot reasonably be used in any way to make determinations about individuals. One may infer from the legislative history and other portions of the Act that an objective of this provision is to reduce the possibility of matching and analysis of statistical records with other records to reconstruct individually identifiable records. An accounting of disclosures is not required when agencies publish aggregate data so long as no individual member of the population covered can be identified; for example, statistics on employee turnover rates, sick leave usage rates.

Viewed from the perspective of the recipient agencies, material thus transferred would not constitute records for its purposes.

DISCLOSURE TO THE NATIONAL ARCHIVES

> Subsection (b)(6) "To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value."

Agencies may disclose records to the National Archives of the United States pursuant to Section 2103 of Title 44 of the United States Code which provides for the preservation of records "of historical or other

value". This subsection ((b)(6)) allows not only the transfer of records for preservation but also the disclosure of records to the Archivist to permit a determination as to whether preservation under Title 44 is warranted. See subsections (l)(2) and (l)(3) for a discussion of constraints on the maintenance of records by the Archives.

Records which are transferred to Federal Records Centers for safekeeping or storage do not fall within this category. Such transfers are not considered to be disclosures within the terms of this Act since the records remain under the control of the transferring agency. Federal Records Center personnel are acting on behalf of the agency which controls the records. See subsection (l)(1), below.

DISCLOSURE FOR LAW ENFORCEMENT PURPOSES

> Subsection (b)(7) "To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;"

An agency may, upon receipt of a written request, disclose a record to another agency or unit of State or local government for a civil or criminal law enforcement activity. The request must specify

- the law enforcement purpose for which the record is requested; and
- the particular record requested.

Blanket requests for all records pertaining to an individual are not permitted. Agencies or other entities seeking disclosure may, of course, seek a court order as a basis for disclosure. See subsection (b)(11).

A record may also be disclosed to a law enforcement agency at the initiative of the agency which maintains the record when a violation of law is suspected; provided, that such disclosure has been established in advance as a "routine use" and that misconduct is related to the purposes for which the records are maintained. For example, certain loan or employment application information may be obtained with the understanding that individuals who knowingly and willfully provide inaccurate or erroneous information will be subject

to criminal prosecution. This usage was explicitly addressed by Congressman Moorhead in explaining the House bill, on the floor of the House:

> "It should be noted that the 'routine use' exception is in addition to the exception provided for dissemination for law enforcement activity under subsection (b)(7) of the bill. Thus a requested record may be disseminated under either the 'routine use' exception, the 'law enforcement' exception, or both sections, depending on the circumstances of the case." (Congressional Record November 21, 1974, p.H10962.)

In that same discussion, additional guidance was provided on the term "head of the agency" as that term is used in this subsection ((b)):

> "The words 'head of the agency' deserve elaboration. The committee recognizes that the heads of Government departments cannot be expected to personally request each of the thousands of records which may properly be disseminated under this subsection. If that were required, such officials could not perform their other duties, and in many cases, they could not even perform record requesting duties alone. Such duties may be delegated, like other duties, to other officials, when absolutely necessary but never below a section chief, and this is what is contemplated by subsection (b)(7). The Attorney General, for example, will have the power to delegate the authority to request the thousands of records which may be required for the operation of the Justice Department under this section."

It should be noted that this usage is somewhat at variance with the use of the term "agency head" in subsections (j), and (k), rules and exemptions, where delegations to this extent are neither necessary nor appropriate.

This subsection permits disclosures for law enforcement purposes only to governmental agencies "within or under the control of the United States." Disclosures to foreign (as well as to State and local) law enforcement agencies may, when appropiate, be established as "routine uses."

Records in law enforcement systems may also be disclosed for law enforcement purposes when that disclosure has properly been established as a "routine use"; e.g., statutorily authorized responses to properly made queries to the National Driver Register; transfer by

a law enforcement agency of protective intelligence information to the Secret Service.

DISCLOSURE UNDER EMERGENCY CIRCUMSTANCES

> Subsection (b)(8) "To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;"

Agencies may disclose records when, for example, the time required to obtain the consent of the individual to whom the record pertains might result in a delay which could impair the health or safety of an individual; as in the release of medical records on a patient undergoing emergency treatment. The individual pertaining to whom records are disclosed need not necessarily be the individual whose health or safety is at peril; e.g., release of dental records on several individuals in order to identify an individual who was injured in an accident.

DISCLOSURE TO THE CONGRESS

> Subsection (b)(9) "To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;"

This language does not authorize the disclosure of a record to members of Congress acting in their individual capacities without the consent of the individual.

DISCLOSURE TO THE GENERAL ACCOUNTING OFFICE

> Subsection (b)(10) "To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;"

DISCLOSURE PURSUANT TO COURT ORDER

> Subsection (b)(11) "Pursuant to the order of a court of competent jurisidiction."

Subsection (c)

ACCOUNTING OF CERTAIN DISCLOSURES

Subsection (c) "Each agency, with respect to each system of record under its control, shall--"

WHEN ACCOUNTING IS REQUIRED

Subsection (c)(1) "Except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of--

"(A) The date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

"(B) The name and address of the person or agency to whom the disclosure is made;"

An accounting is required

- for disclosures outside the agency even when such disclosure is at the request of the individual with the written consent or at the request of the individual;
- for disclosures for routine uses (see (b)(3));
- for disclosures to the Bureau of the Census (see (b)(4));
- for disclosures to a person or another agency for statistical research or reporting purposes (see (b)(5));
- for disclosures to the Archives (see (b)(6));
- for disclosures for a law enforcement activity consistent with the provisions of subsection (see (b)(7));
- for disclosures upon a showing of "compelling circumstances" (see (b)(8));
- for disclosures to the Congress or the Comptroller General (see (b)(9) and (10)); or
- for disclosures pursuant to a court order (see (b)(11)).

An accounting of disclosures is not required

- for disclosures to employees of the agency maintaining the record who have a need to have access in the performance of their official duties for the agency. (Agencies are required to establish safeguards, pursuant to subsection (e)(10), to assure that individuals who do not have a "need to know" will not have access.) (see (b)(1)); or

- for disclosures to members of the public which would be required under the Freedom of Information Act (see (b)(2)).

(Note that the accounting requirement is not one from which an agency may seek an exemption under subsections (j) and (k)).

"The term 'accounting' rather than 'record,' [was used] to indicate that an agency need not make a notation on a single document of every disclosure of a particular record. The agency may use any system it desires for keeping notations of disclosures, provided that it can construct from its system a document listing of all disclosures." (House Report 93-1416, p. 14). For example, if a list of names and other pertinent data necessary to issue payroll or benefit checks is transferred to a disbursing office outside the agency, the agency transferring the record need not maintain a separate record of such transfer in each individual record provided that it can construct the required accounting information when requested by the individual (subsection (c)(3)) or when necessary to inform previous recipients of any corrected or disputed information (subsection (c)(4)). The accounting should also provide a cross-reference to the basis upon which the release was made including any written documentation as is required in the case of the release of records for statistical or law enforcement purposes.

In some instances, (e.g., investigation or prosecution of suspected criminal activity) a disclosure may consist of a continuing dialogue between two agencies over a period of weeks or months. In such a situation, it may be appropriate to make a general notation that, as of a specified date, such contact was initiated and will be maintained until the conclusion of the case.

While the accounting of disclosures, when maintained apart from the record, might be considered a system of records under the Act, this could lead to the situation of having to maintain an accounting of disclosures from the original accounting and having to maintain that second accounting for five years, etc. Note that subsection (c)(3) gives an individual a right of access to the accounting which would not have been necessary if the accounting were considered a separate system of record. Therefore, it would seem that the intent was to view the accounting of disclosures as other than a system of records and to conclude that an accounting need not be maintained for disclosures from the accounting of disclosures.

RETAINING THE ACCOUNTING OF DISCLOSURES

Subsection (c)(2) "Retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;"

The purposes of the accounting are (1) to allow individuals to learn to whom records about themselves have been disclosed (subsection (c)(3)); (2) to provide a basis for subsequently advising recipients of records of any corrected or disputed records (subsection (c)(4)); and (3) to provide an audit trail for subsequent reviews of agency compliance with subsection (b) (conditions of disclosure). As discussed above, with respect to maintaining the accounting, the accounting need not be retained on a record by record basis as long as the procedures adopted by the agency permit it to satisfy these objectives. While the accounting is required to be maintained for at least five years, nothing in the Act requires the retention of the record itself where the record could otherwise lawfully be disposed of sooner.

The accounting is required to be retained for five years from the date of the disclosure unless the record is retained longer. Record retention standards remain as prescribed in applicable law and GSA regulations.

MAKING THE ACCOUNTING OF DISCLOSURES AVAILABLE TO THE INDIVIDUAL

> Subsection (c)(3) "Except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request;"

Upon request of the individual to whom the record pertains an agency must make available to that individual all information in its accounting of disclosures except those pertaining to disclosures to another agency or government instrumentality for law enforcement purposes pursuant to subsection (b)(7) unless the system has been exempted from this provision pursuant to subsections (j) or (k). Agencies may wish to maintain the accounting of disclosure in such a manner that notations of disclosures pursuant to (b)(7) are readily segregable in order to facilitate timely release of the disclosure accounting when requested by the individual. Since the accounting will often not be maintained in a form which is readily comprehensible to the individual, the process of "making the accounting available" may entail some transformation of the accounting by the agency so as to make it intelligible to the individual. This may require the agency to compile, from the accounting, a list of those to whom the record was disclosed.

INFORMING PRIOR RECIPIENTS OF CORRECTED OR DISPUTED RECORDS

> Subsection (c)(4) "Inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that

has been disclosed to the person or agency if an accounting of the disclosure was made."

When a record is corrected at the request of an individual acting in accordance with subsection (d)(2) or a statement of dispute is filed as provided in subsection (d)(3), the agency maintaining the record shall notify each agency or person to which the record has been disclosed of the exact nature of the correction or that a notation of dispute has been made. If the recipient was another agency, that agency is required, in turn,to notify those to whom it disclosed the record.

This requirement does not apply to disclosures to personnel within the agency with a "need to know" or to the public under the Freedom of Information Act (subsections (b)(1) and (2)) or to disclosures made prior to September 27, 1975 for which no accounting was made. (Note that the language in subsection (c)(4) differs from the corresponding language in H.R. 16373 so that the House report discussion of this provision is no longer applicable).

Given the definition of "record" (a record may be construed to be a part of another record) and the language of subsection (d)(4), below, it would appear that the notification of correction or of the filing of a statement of disagreement is required only to the extent that the correction or disagreement pertains to the information actually disclosed; i.e., recipients of a portion of a record other than the portion which is subsequently corrected or disputed need not be informed. Where there is any doubt as to whether the corrected information was included in or might be relevant to a previous disclosure, agencies should notify the recipients in question.

The language of this subsection explicitly requires only that prior recipients be notified of corrections made pursuant to a request to amend a record by an individual and does not address records corrected for other reasons; e.g., agency staff detects erroneous data or a third party source provides corrected information. Nevertheless, agencies are encouraged to provide corrected information to previous recipients, irrespective of the means by which the correction was made whenever it is deemed feasible to do so if information included in a previous disclosure was changed particulary when the agency is aware that the correction is relevant to the recipient's uses irrespective of the means by which the correction is made.

Subsection (d)

ACCESS TO RECORDS

Subsection (d) "Each agency that maintains a system of record shall--"

INDIVIDUAL ACCESS TO RECORDS

Subsection (d)(1) "Upon request by an individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;"

An agency must, upon request; (1) inform an individual whether a system of records contains a records or records pertaining to him, (2) permit an individual to review any record pertaining to him which is contained in a system of records, (3) permit the individual to be accompanied for the purpose by a person of his choosing, and (4) permit the individual to obtain a copy of any such record in a form comprehensible to him at a reasonable cost. This provision it should be noted, gives an individual the right of access only to records which are contained in an system of records. See (a)(5), above.

This language further suggests that the Congress did not intend to require that an individual be given access to information which the agency does not retrieve by reference to his or her name or some other identifying particular. See subsection (a)(5). If an individual is named in a record about someone else (or some other type of entity) and the agency only retrieves the portion pertaining to him by reference to the other person's name (or some organization/subject identifier), the agency is not required to grant him access. Indeed, if this were not the case, it would be necessary to establish elaborate cross-references among records, thereby increasing the potential for privacy abuses. The following examples illustrate some applications of this standard.

1. A record on Joan Doe as an employee in a file of employees from which material is accessed by reference to her name (or some identifying number). This is the simplest case of a record in a system of records and Joan Doe would have a right of access.

2. A reference to Joan Doe in a record about James Smith in the same file. This is also a record within a system but Joan Doe would not

63-619 O - 76 - 67

have to be granted access unless the agency had devised and used an indexing capability to gain access to her record in James Smith's file.

3. A record about Joan Doe in a contract source evaluation file about her employer, Corporation X, which is not accessed by reference to individuals' names, or other indentifying particulars. This is a record which is not in a system of records and, therefore, Joan Doe would not have a right of access to it. If, as in 2, above, an indexing capability were developed and used, however, such a system would become a system of records to which Joan Doe would have a right of access.

Agencies may establish fees for making copies of an individual's record but not for the cost of searching for a record or reviewing it (subsection (f)(5)). When the agency makes a copy of a record as a necessary part of its process of making the record available for review (as distinguished from responding to a request by an individual for a copy of a record), no fee may be charged. It should be noted that this provision differs from the access and fees provisions of the Freedom of Information Act.

The granting of access may not be conditioned upon any requirement to state a reason or otherwise justify the need to gain access.

Agencies shall establish requirements to verify the identity of the requestor. Such requirements shall be kept to a minimum. They shall only be established when necessary reasonably to assure that an individual is not improperly granted access to records pertaining to another individual and shall not unduly impede the individual's right of access. Procedures for verifying identity will vary depending upon the nature of the records to which access is sought. For example, no verification of identity will be required of individuals seeking access to records which are otherwise available to any member of the public under 5 U.S.C. 552, the Freedom of Information Act. However, far more stringent measures should be utilized when the records sought to be accessed are medical or other sensitive records.

For individuals who seek access in person, requirements for verification of identity should be limited to information or documents which an individual is likely to have readily available (e.g., a driver's license, employee identification card, Medicare card). However, if the individual can provide no other suitable documentation, the agency should request a signed statement from the individual asserting his or her identity and stipulating that the individual understands that knowingly or willfully seeking or obtaining access to records about another individual under false pretenses is punishable by a fine of up to $5,000. (Subsection (i)(3)).

For systems to which access is granted by mail (by virtue of their location) verification of identity may consist of the providing of

certain minimum identifying data; e.g., name, date of birth, or system personal identifier (if known to the individual). Where the sensitivity of the data warrants it; (i.e., unauthorized access could cause harm or embarrassment to the individual), a signed notarized statement may be required or other reasonable means of verifying identity which the agency may determine to be necessary, depending on the degree of sensitivity of the data involved.

Note that section 7 of the Act forbids an agency to deny an individual any right (including access to a record) for refusing to disclose a Social Security Number unless disclosure is required by Federal statute or by other laws or regulations adopted prior to January 1, 1975.

Agencies are also permitted to require that an individual who wishes to be accompanied by another person when reviewing a record furnish a written statement authorizing discussion of his or her record in the presence of the accompanying person. This provision may not be used to require that individuals who request access and wish to authorize other persons to accompany them provide any reasons for the access or for the accompanying person's presence. It is designed to avoid disputes over whether the individual granted permission for disclosure of information to the accompanying person.

Agency procedures for complying with the individual access provisions will necessarily vary depending upon the size and nature of the system of records. Large computer-based systems of records clearly require a different approach than do small, regionally dispersed, manually maintained systems. Nevertheless the basic requirements are constant, namely the right of the individual to have access to a record pertaining to him and to have a copy made of all or any portion of such records in a form which is comprehensible to him. Putting information into a comprehensible form suggests converting computer codes to their literal meaning but not necessarily an extensive tutorial in the agency's procedures in which the record is used.

Neither the requirements to grant access nor to provide copies necessarily require that the physical record itself be made available. The form in which the record is kept (e.g., on magnetic tape) or the context of the record (e.g., access to a document may disclose records about other individuals which are not relevant to the request) may require that a record be extracted or translated in some manner; e.g., to expunge the identity of a confidential source. Whenever possible, however, the requested record should be made available in the form in which it is maintained by the agency and the extraction or translation process may not be used to withhold information in a record about the individual who requests it unless the denial of access is specifically provided for under rules issued pursuant to one of the exemption provisions (subsections (j) and (k)).

Subsection (f)(3) provides that agencies may establish "a special procedure, if deemed necessary," for the disclosure to an individual of medical records, including psychological records, pertaining to him." In addressing this provision the House committee said:

"If, in the judgment of the agency, the transmission of medical information directly to a requesting individual could have an adverse effect upon such individual, the rules which the agency promulgates should provide means whereby an individual who would be adversely affected by receipt of such data may be apprised of it in a manner which would not cause such adverse effects. An example of a rule serving such purpose would be transmission to a doctor named by the requesting individual." (House Report 93-1416, pp. 16-17)

Thus, while the right of individuals to have access to medical and pychological records pertaining to them is clear, the nature and circumstances of the disclosure may warrant special procedures.

While the Act provides no specific guidance on this subject, agencies should acknowledge requests for access to records within 10 days of receipt of the request (excluding Saturdays, Sundays, and legal public holidays). Wherever practicable, that acknowledgement should indicate whether or not access can be granted and, if so, when. When access is to be granted, agencies will normally provide access to a record within 30 days (excluding Saturdays, Sundays, and legal public holidays) unless, for good cause shown, they are unable to do so, in which case the individual should be informed in writing within 30 days as to those reasons and when it is anticipated that access will be granted. A "good cause" might be the fact that the record is inactive and stored in a records center and, therefore, not as readily accessible. See subsection (l)(1). Presumably, in such cases the risk of an adverse determination being made on the basis of a record to which access is sought and which the individual might choose to challenge is relatively low.

REQUESTS FOR AMENDING RECORDS

Subsection (d)(2) "Permit the individual to request amendment of a record pertaining to him and--"

Agencies shall establish procedures to give individuals the opportunity to request that their records be amended. The procedures may permit the individual to present a request either in person, by telephone, or through the mail but the process should not normally require that the individual present the request in person. If the agency deems it appropriate, it may require the requests be made in writing, whether presented in person or through the mail. Instructions for the preparation of a request and any forms employed should be as brief and as simple as possible. If a request is received on other than a prescribed form, the agency should not reject it or request resubmission unless additional information is essential to process the request. In that case, the inquiry to the individual should be limited to obtaining the needed additional information, not

resubmission of the entire request. Incomplete or inaccurate requests should not be rejected categorically. The individual should be asked to clarify the request as needed. Requests presented in person should be screened briefly while the individual is still present, wherever possible, to assure that the request is complete so that clarification may be obtained on the spot.

These provisions for amending records are not intended to permit the alteration of evidence presented in the course of judicial, quasi-judicial or quasi-legislative proceedings. Any changes in such records should be made only through the established procedures consistent with the adversary process. These provisions are not designed to permit collateral attack upon that which has already been the subject of a judicial or quasi-judicial action. For example, these provisions are not designed to permit an individual to challenge a conviction for a criminal offense received in another forum or to reopen the assessment of a tax liability, but the individual would be able to challenge the fact that conviction or liability has been inaccurately recorded in his records.

The agency should also require verification of identity to assure that the requestors are seeking to amend records pertaining to themselves and not, inadvertently or intentionally, the records of other individuals.

ACKNOWLEDGEMENT OF REQUESTS TO AMEND RECORDS

> Subsection (d)(2)(A) "Not later than 10 days (excluding, Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and"

A written acknowledgement by the agency of the receipt of a request to amend a record must be provided to the individual within 10 days (excluding Saturdays, Sundays, and legal public holidays). The acknowledgement should clearly describe the request (a copy of the request form may be appended to the acknowledgement) and advise the individual when he or she may expect to be advised of action taken on the request.

No separate acknowledgement of receipt is necessary if the request can be reviewed, processed, and the individual advised of the results of the review (whether complied with or denied) within the 10-day period.

For requests presented in person, written acknowledgement should be provided at the time the request is presented.

ACTIONS REQUIRED ON REQUESTS TO AMEND RECORDS

Subsection (d)(2)(B) "Promptly, either

"(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

"(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of the refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;"

In reviewing an individual's request to amend a record, agencies should, wherever practicable, complete the review and advise the individual of the results within 10 days of the receipt of the request. Prompt action is necessary both to assure that records are as accurate as possible and to reduce the administrative effort which would otherwise be involved in issuing a separate acknowledgement of the receipt of the request and subsequently informing the individual of the action taken. If the nature of the request or the system of records precludes completing the review within 10 days, the required acknowledgement (subsection (d)(2)(A) above,) must be provided within ten days and the review should be completed as soon as reasonably possible, normally within 30 days from the receipt of the request (excluding Saturdays, Sundays, and legal public holidays) unless unusual circumstances preclude completing action within that time. (The number of cases on which the agency was unable to act within 30 days will be included in the annual report (subsection (p)). If the expected completion date for the review indicated in the acknowledgement cannot be met, the individual should be advised of that delay and of a revised date when the review may be expected to be completed.

"Unusual circumstances" can be viewed as situations in which records cannot be reviewed through the agency's normal process. By definition, such cases would, statistically, be the exception. A review which entails obtaining supporting data from retired records or from another agency and which could not, therefore be completed within the required time might qualify.

In reviewing a record in response to a request to amend it, the agency should assess the accuracy, relevance, timeliness, or completeness of the record in terms of the criteria established in subsection (e)(5), i.e.,to assure fairness to the individual to whom the record pertains in any determination about that individual which may be made on the basis of that record.

With respect to requests to delete information, agencies must heed the criteria established in subsection (e)(1), namely, that the information must be "... relevant and necessary to accomplish a statutory purpose of the agency required to be accomplished by law or by executive order of the President." This is not to suggest that

agencies may routinely maintain irrelevant or unnecessary information unless it is challenged by an individual, but rather that receipt of a request to delete information should cause the agency to reconsider the need for such information. Reviews in connection with the development of a system, the preparation of the public notice and the description of the purposes for which it is maintained and periodic reviews of the system, to assure that only information which is necessary for the lawful purposes for which the system of records was established is maintained in it will be the primary vehicles for assuring that only relevant and necessary information is maintained.

Agency standards for reviewing records in response to a request to amend them may, at the agency's option, be included as part of the rules promulgated pursuant to subsection (f)(4). Generally, it would seem reasonable to conclude that such standards for review need be no more stringent than is reasonably necessary to meet the general criteria in subsections (e)(1) and (e)(5) for accuracy, relevance, timeliness, and completeness.

Judicial review is available for agency determinations to grant an individual access and to amend or not amend a record pertaining to the individual. While the definite burden of proof for granting access is upon the agency in such judicial review, in the judicial review of the refusal of an agency to amend a record there is no similar burden upon the agency. An analogous standard may be utilized by the agencies in establishing standards for review of individual requests for amendments of records. The burden of going forward could be placed upon the individual who in most instances will know better than the agency the reasons why the record should be amended. It would be appropriate, in agency regulations setting forth the standards they will use upon review of such request, that the individual be required to supply certain information in support of his request for amendment of the record. The request would then be appropriate for resolution upon determination of preponderance of evidence.

If the agency agrees with the individual's request to amend a record, the agency shall--

- advise the individual;
- correct the record accordingly; and
- where an accounting of disclosures has been made, advise all previous recipients of the record of the fact that the correction was made and the substance of the correction.

If the agency, after its initial review of a request to amend a record, disagrees with all or any portion thereof, the agency shall

- to the extent that the agency agrees with any part of the individual's request to amend, proceed as described above with respect to those portions of the record which it has amended.

- advise the individual of its refusal and the reasons therefor including the criteria for determining accuracy which were employed by the agency in conducting the review;

- inform the individual that he or she may request a further review by the agency head or by an officer of the agency designated by the agency head; and

- describe the procedures for requesting such a review including the name and address of the official to whom the request should be directed. The procedures should be as simple and brief as possible and should indicate where the individual can seek advice or assistance in obtaining such a review.

If the recipient of the corrected information is an agency and is maintaining the information which was corrected in a system of records, it must correct its records and, under subsection (c)(4), apprise any agency or person to which it had disclosed the record of the substance of the correction. Subsequent recipient agencies should similarly correct their records and advise those to whom they had disclosed it. Agencies are encouraged to establish in their regulations, time limits by which, except under unusual circumstances, transferees of any amendment to a record.

REQUESTING A REVIEW OF THE AGENCY'S REFUSAL TO AMEND A RECORD

> Subsection (d)(3) "Permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review, and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;"

An individual who disagrees with an agency's initial refusal to amend a record may file a request for further review of that determination. The agency head or an officer of the agency designated in writing by the agency head should undertake an independent review of the initial determination. If someone other than the agency head is designated to

conduct the review, it should be an officer who is organizationally independent of or senior to the officer or employee who made the initial determination. For purposes of this section, an "officer" is defined to be "... a justice or judge of the United States and an individual who is--

"(1) required by law to be appointed in the civil [or military]* service by one of the following acting in an official capacity--

[*It is assumed that, while the language above does not specifically cover it, a military officer otherwise qualified as the reviewing official would be permitted to serve as the reviewing official.]

"(A) the President;

"(B) a court of the United States;

"(C) the head of an Executive agency; or

"(D) the Secretary of a military department;

"(2) engaged in the performance of a Federal function under authority of law or an Executive act; and

"(3) subject to the supervision of an authority named by paragraph (1) of this section, or the Judicial Conference of the United States, while engaged in the performance of the duties of his office." (5 U.S.C. 2104(a)).

Delegations must be made in writing. In conducting the review, the reviewing official should use the criteria of accuracy, relevance, timeliness, and completeness discussed above. The reviewing official may, at his or her option, seek such additional information as is deemed necessary to satisfy those criteria; i.e., to establish that the record contains only that information which is necessary and is as accurate, timely, and complete as necessary to assure fairness in any determination which may be made about the individual on the basis of record.

Although there is no requirement for a formal hearing, pursuant to the provisions of 5 U.S.C. 556, the agency may elect generally or on a case by case basis to use such or similar procedures. The procedures elected by the agency, however, should insure fairness to the individual and promptness in the determination. The procedures should provide that as much of the information upon which the determination is based as possible is part of the written record concerning the appeal. The records of the appeal process should be maintained by agencies only as long as is reasonably necessary for purposes of judicial review of the agency's refusal to amend a record upon appeal.

If, after conducting this review, the reviewing official also refuses to amend the record in accordance with the individual's request, the agency shall advise the individual:

- of its refusal and the reasons therefor;

- of his or her right to file a concise statement of the individual's reasons for disagreeing with the decision of the agency;

- of the procedures for filing a statement of disagreement;

- that any such statement will be made available to anyone to whom the record is subsequently disclosed together with, if the agency deems it appropriate, a brief statement by the agency summarizing its reasons for refusing to amend the record;

- that prior recipients of the disputed record will be provided a copy of any statement of dispute to the extent that an accounting of disclosures was maintained (see subsection (c)(4)); and

- of his or her right to seek judicial review of the agency's refusal to amend a record provided for in subsection (g)(1)(A), below.

If the reviewing official determines that the record should be amended in accordance with the individual's request, the agency should proceed as prescribed in subsection (1)(2)(B)(i), above; namely, correct the record, advise the individual, and inform previous recipients.

A notation of a dispute is required to be made only if an individual informs the agency of his or her disagreement with the agency's determination under subsection (d)(3) (appeals procedure) not to amend a record.

A final agency determination on the individual's request for a review of an agency's initial refusal to amend a record must be completed within 30 days unless the agency head determines that a fair and equitable review cannot be completed in that time. If additional time is required, the individual should be informed in writing of the reasons for the delay and of the approproximate date on which the review is expected to be completed. Such extensions should not be routine and should not normally exceed an additional thirty days. Agencies will be required to report the number of cases in which review was not completed within 30 days as part of the annual report (subsection (p)).

DISCLOSURE OF DISPUTED INFORMATION

Subsection (d)(4) "In any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3)

> of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed;"

When an individual files a statement disagreeing with the agency's decision not to amend a record, the agency should clearly annotate the record so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. The notation itself should be integral to the record and specific to the portion in dispute. For automated systems of records, the notation may consist of a special indicator on the entire record or the specific part of the record in dispute.

The statements of dispute need not be maintained as an integral part of the records to which they pertain. They should, however, be filed in such a manner as to permit them to be retrieved readily whenever the disputed portion of the record is to be disclosed.

If there is any question as to whether the dispute pertains to information being disclosed, the statement of dispute should be included.

When information which is the subject of a statement of dispute is subsequently disclosed, agencies must note that the information is disputed and provide a copy of the individual's statement.

Agencies may, at their discretion, include a brief summary of their reasons for not making a correction when disclosing disputed information. Such statements will normally be limited to the reasons stated to the individual under subsection (d)(2)(B)(ii) and (d)(3), above. Copies of the agency's statement need not be maintained as an integral part of the record but will be treated as part of the individual's record for purposes of granting the individual access, subsection (d)(1). However, the agency's statement will not be subject to subsections (d)(2) or (3) (amending records).

ACCESS TO INFORMATION COMPILED IN ANTICIPATION OF CIVIL ACTION

> Subsection (d)(5) "Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding."

This provision is not intended to preclude access by an individual to records which are available to that individual under other procedures (e.g., pre-trial discovery). It is intended to preclude establishing

by this Act a basis for access to material being prepared for use in litigation other than that established under other processes such as the Freedom of Information Act or the rules of civil procedure.

Excerpts from the House floor debate on this provision suggest that this provision was not intended to cover access to systems of records compiled or used for purposes other than litigation.

> "Mr. ERLENBORN. Mr. Chairman, as I understand it, the purpose of the amendment is to protect, as an example, the file of the U.S. attorney or the solicitor that is prepared in anticipation of the defense of a suit against the United States for accident or some such thing?
>
> "Mr. BUTLER. That is the subject we have in mind.
>
> "Mr. ERLENBORN. I appreciate the gentleman's concern. I think it is a real concern, and that protection ought to be afforded.
>
> "The only problem I find with that amendment is this: It would presuppose we intended the defining of 'record system' to preclude that type of record. I do not think we did.
>
> "If these sorts of records are to be considered a record system under the act, then the agency would have to go through all the formal proceedings of defining the system, its routine uses, and publishing in the Federal Register .
>
> "Frankly, I do not think the attorney's files that are collected in anticipation of a lawsuit should be subject to the application of the act in any instance, much less the access provision. It is our concern in the access provision that it may then presuppose it is covered in the other provisions, and I do not think it should be.
>
> "Mr. BUTLER. Mr. Chairman, I share the gentleman's concern. When this amendment was originally drafted, it stated 'access to any record' and we struck the word, "record," and inserted 'information.'
>
> "So we made it perfectly clear we were not elevating an investigation with the word, 'record,' to the status of records. We did want to make it clear there was not to be such access, because that access would be within the usual rules of civil procedure.
>
> "Mr. ERLENBORN. Mr. Chairman, if the gentleman will yield further, it is the gentleman's contention, under his interpretation of the act, that the other provisions would not apply to the attorney's files as well; is that correct?
>
> "Mr. BUTLER. The gentleman is correct." (Congressional Record , November 21, 1974 p. H10955).

While the above passage refers primarily to the defense of suits by the government it is, of course, equally applicable to the assembly of information in anticipation of government-initiated law suits.

The mere fact that records in a system of records are frequently the subject of litigation does not bring those systems of records within the scope of this provision. The information must be "compiled in reasonable anticipation of a civil action or proceeding" and therefore the purpose of the compilation governs the applicability of this provision. It would seem that in a suit in which governmental action or inaction is challenged the provision generally would not be available until the initiation of litigation or until information began to be compiled in reasonable anticipation of such litigation. Where the government is prosecuting or seeking enforcement of its laws or regulations, this provision may be applicable at the outset if information is being compiled in reasonable anticipation of a civil action or proceeding. The term civil proceeding was intended to cover those quasi-judicial and preliminary judicial steps which are the counterpart in the civil sphere of criminal proceedings as opposed to criminal litigation. Although this provision could have the effect of an exemption it is not subject to the formal rule-making procedures which govern the exemptions set forth in subsection (j) and (k). Nevertheless, agencies should utilize the specific exemptions set forth in subsections (j) and (k) to the extent that they are applicable before utilizing this provision.

Section (e)

AGENCY REQUIREMENTS

Section (e) "Each agency that maintains a system of records shall--"

RESTRICTIONS ON COLLECTING INFORMATION ABOUT INDIVIDUALS

Subsection (e)(1) "Maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;"

A key objective of the Act is to reduce the amount of personal information collected by Federal agencies to reduce the risk of intentionally or inadvertently improper use of personal data. In simplest terms, information not collected about an individual cannot be misused. The Act recognizes, however, that agencies need to maintain information about individuals to discharge their responsibilities effectively.

Agencies can derive authority to collect information about individuals in one of two ways:

- by the Constitution, a statute, or Executive order explicitly authorizing or directing the maintenance of a system of records; e.g., the Constitution and title 13 of the United States Code with respect to the Census.

- by the Constitution, a statute, or Executive order authorizing or directing the agency to perform a function, the discharging of which requires the maintenance of a system of records.

Each agency shall, with respect to each system of records which it maintains or proposes to maintain, identify the specific provision in law which authorizes that activity. While the Act does not specifically require it, where feasible, this statutory authority should also be cited in the annual public notice about the system published pursuant to subsection (e)(4). The authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful. Agencies shall review the nature of the information which they maintain in their systems of records to assure that it is, in fact, "relevant and necessary". Information may not be maintained merely because it is relevant; it must be both relevant and necessary. While this determination is, in the final analysis, judgmental, the following types of questions shall be considered in making such determinations:

- How does the information relate to the purpose (in law) for which the system is maintained?

- What are the adverse consequences, if any, of not collecting that information?

- Could the need be met through the use of information that is not in individually identifiable form?

- Does the information need to be collected on every individual who is the subject of a record in the system or would a sampling procedure suffice?

- At what point will the information have satisfied the purpose for which it was collected; i.e., how long is it necessary to retain the information? Consistent with the Federal Records Act and related regulations could part of the record be purged?

- What is the financial cost of maintaining the record as compared to the risks/adverse consequences of not maintaining it?

- Is the information, while generally relevant and necessary to accomplish a statutory purpose, specifically relevant and necessary only in certain cases? For example in establishing financial need as part of assessing eligibility for a program for which need is a legitimate criterion, parental income may be relevant only for certain applicants.

Subsection (e)(7), below, provides additional criteria governing the maintenance of records on the activities of individuals in exercising their rights under the First Amendment.

This provision does not authorize agencies to destroy records which they are required to retain under the Federal Records Act.

Agencies shall assess the legality of, need for, and relevance of the information contained or proposed to be contained in each of its systems of records at various times:

- In preparing initial public notices (subsection (e) (4)).

- In connection with the initial design of a new system of records (subsection (o)).

- Whenever any change is proposed in the information content of an existing system of records (subsection (o)).

- At least annually, as part of a regular program of review of its record-keeping practices. This should be done for each system prior to reissuance of the public notice unless a comprehensive review of the system of records was conducted within the previous year in connection with the initiation of the system or implementation of a change to the system.

This provision does not require that each agency conduct a detailed review of the contents of each record in its possession. Rather, agencies shall consider the relevance of, and necessity for, the general categories of information maintained and, incident to using or

disclosing any individual records, examine their content to assure compliance with this provision.

It should be noted that subsection (e) is not intended to interfere with the presentation of evidence by the parties before a quasi-judicial or quasi-legislative body. For example, a quasi-judicial board or commission need not reject otherwise admissible evidence because it is proffered by a part other than the individual to whom it relates or because it is not "neccessary" to the decision or is not "complete." The normal rules of evidence would contains to govern in such situations.

INFORMATION IS TO BE COLLECTED DIRECTLY FROM THE INDIVIDUAL

> Subsection (e)(2) "Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs;"

This provision stems from a concern that individuals may be denied benefits, or that other adverse determinations affecting them may be made by Federal agencies on the basis of information obtained from third party sources which could be erroneous, outdated, irrelevant, or biased. This provision establishes the requirement that decisions under Federal programs which affect an individual should be made on the basis of information supplied by that individual for the purpose of making those determinations but recognizes the practical limitations of this by qualifying the requirement with the words " to the extent practicable". The notion of protecting the individual against adverse determinations based on information supplied to other agencies for other purposes is also embodied in the provisions of subsection (b) which constrains the transfer of records between agencies; subsection (d)(2), which gives individuals the opportunity to challenge the accuracy of agency records pertaining to them; and subsection (e)(4) which prohibits the keeping of secret files.

Except for certain "statistical records" (subsection (a)(6)), which, by definition, are "not used in whole or in part in making a determination about an individual...", virtually any other record could be used, in making a "determination about an individual's rights, benefits, or privileges..." including employment. The practical effect of this provision is to require that information collected for inclusion in any system of records, other than "statistical records", should be obtained directly from the individual whenever practicable.

Practical considerations (including cost) may dictate that a third-party source, including systems of records maintained by another agency, be used as a source of information in some cases. In

analyzing each situation where it proposes to collect personal information from a third party source, agencies should consider

- the nature of the program; i.e., it may well be that the kind of information needed can only be obtained from a third party such as investigations of possible criminal misconduct;

- the cost of collecting the information directly from the individual as compared with the cost of collecting it from a third party;

- the risk that the particular elements of information proposed to be collected from third parties, if inaccurate, could result in an adverse determination;

- the need to insure the accuracy of information supplied by an individual by verifying it with a third party or to obtain a qualitative assessment of his or her capabilities (e.g., in connection with reviews of applications for grants, contracts or employment); and

- provisions for verifying, whenever possible, any such third-party information with the individual before making a determination based on that information.

It should be noted that a determination by Agency (A) that it is in its best interest and consistent with this subsection to obtain information about an individual from Agency (B) instead of directly from the individual does not constitute, in and of itself, sufficient grounds for Agency (B) to release that information to Agency (A). Agency (B) is minimally required to meet the requirements of any statutory constraints on the permissibility of making a disclosure to Agency (A) including the conditions of disclosure, in subsection (b).

The standards and procedures set forth in the Federal Reports Act (44 USC 3501) as they apply to other than individuals as defined by this Act remain the same. When information is sought, however, from ten or more individuals, as defined by the Privacy Act, in response to identical questions, the Federal Reports Act requirement that the reporting burden upon individuals be reduced to a minimum should not be construed to override the later enacted requirement that, to the greatest practicable extent, information pertaining to individuals be collected directly from them.

INFORMING INDIVIDUALS FROM WHOM INFORMATION IS REQUESTED

> Subsection (e)(3) "Inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual--"

This provision is intended to assure that individuals from whom information about themselves is collected are informed of the reasons

63-619 O - 76 - 68

for requesting the information, how it may be used, and what the consequences are, if any, of not providing the information.

Implicit in this subsection is the notion of informed consent since an individual should be provided with sufficient information about the request for information to make an informed decision on whether or not to respond. Note however, that the act of informing the individual of the purpose(s) for which a record may be used does not, in and of itself, satisfy the requirement to obtain consent for disclosing the record. See subsection (b),conditions of disclosure.

The information called for in paragraphs (A) through (D) below, should be included on the information collection form, on a tear-off sheet attached to the form, or on a separate sheet which the individual can retain, whichever is most practical. When information is being collected in an interview, the interviewer should provide the individual with a statement that the individual can retain. However, the interviewer should also orally summarize that information before the interview begins. Agencies may, at their discretion, ask the individuals to acknowledge in writing that they have been duly informed.

While this provision does not explicitly require it, agencies should, where feasible, inform third-party sources of the purposes for which information which they are asked to provide will be used. In addition, the agency may, under certain circumstances, assure a source that his or her identity will not be revealed to the subject of the record (see subsection (k)(2), (5), and (7)). The appropriate use of third-party sources is discussed in subsection (e)(2) above.

In providing the information required by subsections (e)(3)(A) through (D), below, care should be exercised to assure that easily understood language is used and that the material is explicit and informative without being so lengthy as to deter an individual from reading it. Information provided pursuant to this requirement would not, for example, be as extensive as that contained in the system notice (subsection (e)(4)).

It was not the intent of this subsection to create a right the nonobservance of which would preclude the use of the information or void an action taken on the basis of that information. For example, a failure to comply with this section, in collecting crop yield data from a farmer, was not intended to vitiate a crop import quota based, in part, upon such information. However, such an individual may have grounds for civil action under subsection (g)(1)(D) if he can show harm as a result of that determination.

> Subsection (e)(3)(A)"The authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;"

The agency should cite the specific provision in statute or Executive order which authorizes the agency to collect the requested information (see subsection (e)(1) above), the brief title or subject of that

statute or order, and whether or not the collecting agency is required to impose penalties for failing to respond or is authorized to impose penalties. Where the system is maintained pursuant to some more general requirement or authority, it should be cited. The question of whether compliance is mandatory or voluntary is different from the question of whether there are any consequences of not providing information; i.e., the law may not require individuals to apply for a benefit but clearly, for some types of voluntary programs, to apply without supplying certain minimal information might preclude an agency from making an informed judgment and thereby prevent an individual from obtaining a benefit. (See subsection (e)(3)(D) regarding the requirement to inform individuals of the effects, if any, of not providing information.)

In some instances it may be necessary to include required and optional information on the same data collection form. This should be avoided to the extent possible since the likely effect on some respondents may be coercive; i.e., they may fear that, even though portions of an information request are voluntary, by failing to respond, they may be perceived to be uncooperative and their opportunities would thereby be prejudiced. (See 44 U.S.C. 3511, the Federal Reports Act).

> Subsection (e)(3)(B)"The principal purpose or purposes for which the information is intended to be used;"

The individual should be informed of the principal purpose(s) for which the information will be used; e.g., to evaluate suitability, to issue benefit payments. The description of purpose(s) must include all major purposes for which the record will be used by the agency which maintains it and particularly those likely to entail determinations as to the individual's rights, benefits, etc. As in all other portions of the information collection process, purposes should be stated with sufficient specificity to communicate to an individual without being so lengthy as to discourage reading of the notice. Generally, the purposes will be directly related to, and necessary for, the purpose authorized by the statute or executive order cited above.

> Subsection (e)(3)(C) "The routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and"

"Uses" can be distinguished from "purposes" in that "purposes" describe the objectives for collecting or maintaining information, whereas "uses" are the specific ways or processes in which the information is employed including the persons or agencies to whom the record may be disclosed. For example, the purposes for collecting information may be to evaluate an application for a veterans' benefit and issue checks. Uses might include verification of certain information with the Department of Defense and release of check-issue data to the Treasury Department, or disclosure to the Justice Department that the applicant apparently intentionally provided false or misleading information.

The term "routine use" is defined in subsection (a)(7) to mean the disclosure of a record "...for a purpose which is compatible with the purpose for which it was collected." A "routine use" is one which is relatable and necessary to a purpose described pursuant to subsection (e)(3)(B), and involves disclosure outside the agency which maintains the record. "Routine uses" must be included not only in the public notice about the system of records published in accordance with subsection (e)(4), below, but also established in advance by notice in the Federal Register to permit public comment. See subsection (e)(11), below.

The description of "routine uses" provided to the individual at the time information is collected will frequently be a summary of the material published in the public notice pursuant to subsection (e)(4)(D). As with other portions of the notification to the individual, care should be exercised to tailor the length and tone of the notice to the circumstances; i.e., the public notice published pursuant to subsection (e)(4) can be much more detailed than the notice to the individual appended to an information collection form.

> Subsection (e)(3)(D) "The effects on him, if any, of not providing all or any part of the requested information;"

The intent of this subsection is to allow an individual from whom personal information is requested to know the effects (beneficial and adverse), if any, of not providing any part or all of the requested information so that he or she can make an informed decision as to whether to provide the information requested on an information collection form or in an interview.

The individual should be informed of the effects, if any, of not responding. This should be stated in a manner which relates to the purposes for which the information is collected; e.g., the information is needed to evaluate disabled veterans for special counseling and training and if it is not provided, no additional training will be considered but disability annuities payments will continue. Particular care must be exercised in the drafting of the wording of the notice to assure that the respondent to the information request is not misled or inadvertently coerced.

PUBLICATION OF THE ANNUAL NOTICE OF SYSTEMS OF RECORDS

> Subsection (e)(4) "Subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include--"

The public notice provision is central to the achievement of one of the basic objectives of the Act; fostering agency accountability through a system of public scrutiny. The public notice provision is premised on the concept that there should be no system of records whose very existence is secret.

The purposes of the notice are to inform the public of the existence of systems of records;

- the kinds of information maintained;
- the kinds of individuals on whom information is maintained;
- the purposes for which they are used;and
- how individuals can exercise their rights under the Act.

All systems of records maintained by an agency are subject to the annual public notice requirement. (The general and special exemption sections permit agencies to omit portions of the notice for certain systems. They do not exempt any agency from publishing a public notice on any system of records).

Care must be exercised to assure that the tone, language, level of detail and length of the public notice are considered to assure that the notice achieves the objective of informing the public of the nature and purposes of agency systems of records.

Defining what constitutes a "system" for purposes of preparing a notice will be left to agency discretion within the general guidelines contained herein. (See also subsection (a)(5)). A system can be a small group of records or, conceivably, the entire complex of records used by an agency for a particular program. Several factors bear on the determination by the agency as to what will constitute a system:

- If each small grouping of records is treated as a separate system, then public notices and procedures will be required for each. The publication of numerous notices may have the effect of limiting the information value to the public.
- If a large complex of records is treated as a single system, only one notice will be required but that notice and the procedures may be considerably more complex.
- Agencies can expect to be required to respond to individual requests for access to records pertaining to them at the level of detail in their public notices, i.e., if an agency treats its records for a particular program as a single system, it may be called upon by an individual to be given access to all information in records pertaining to that individual in the system.
- The purpose(s) of a system is the most important criterion in determining whether a system is to be treated as a single system or several systems for the purposes of the Act. If each of several groupings of agency records is used for a unique purpose or set of purposes, as delineated in subsection (e)(3)(B) above, each may appropriately be treated as a separate system. Agencies should keep in mind that a major purpose of the Act is not the restructuring of existing systems of records, but rather the publicizing of what those systems are and how they are used. It

does not, of course, preclude such restructuring where otherwise necessary or appropriate such as to reduce the risk of improper access.

- Geographic decentralization will not in and of itself be considered a criterion for viewing a system of records as several systems. An agency may treat a decentralized system as a single system and specify several locations and an agency official responsible for the system at each location. See subsections (e)(4)(A) and (F). While the development of central indexes for systems which do not presently require such indexes should be avoided wherever possible, individuals who seek to learn whether a geographically decentralized system of records contains a record pertaining to them (subsection (f) (1)) should not be required to query each location. (In deciding whether or not to construct an index, agencies must weigh the potential threat of misuse posed by making individual records more accessible against the capability to meet the needs of those individuals for access to their records). It may, however, be possible to guide individuals as to which location may have a record pertaining to them; e.g., systems segmented by location of birth, or by range of identification number. In any case, "if a system is located in more than one place, each location must be listed." (House Report 93-1416, p.15) See subsection (e) (4) (A).

A major criterion in determining whether a grouping of records constitutes one system or several, for purposes of the Act, will be the ability to be responsive to the requests of the individual for access to records and generally to be informed.

Systems, however, should not be subdivided or reorganized so that information which would otherwise have been subject to the act is no longer subject to the act. For example, if an agency maintains a series of records not arranged by name or personal identifier but uses a separate index file to retrieve records by name or personal identifier it should not treat these files as separate systems.

A public notice is required to be published:

- for each system in operation on September 27, 1975 on or prior to that date and the notice shall be republished, including any revisions, on or before August 30, each year thereafter.

- for new systems, before the system of records becomes operational; i.e., before any information about individuals is collected.

It should be noted that each "routine use" of a system must have been established in a notice published for public comment at least 30 days prior to the disclosure of a record for that "routine use" as specified in subsection (e)(11).

For major changes to existing systems, a revised public notice is required before that change is effective. If the change to an existing system involves changes to "routine uses", they are subject to the 30

day advance notice provisions of subsection (e)(11). The nature of the changes in a system which would require the issuance of a revised public notice before the next annual public notice is described for each element of the public notice in the succeeding paragraphs. Generally, any change in a system which has the effect of expanding the categories of records maintained, the categories of individuals on whom records are maintained, or the potential recipients of the information, will require the publication of a revised public notice before the change is put into effect. In addition, any modification that alters the procedures by which individuals exercise their rights under the Act (e.g., for gaining access) will require the publication of a revised notice before that change becomes effective.

Changes of the type described above will typically also require the preparation of a "Report on New Systems" under subsection (o), below. Any other change will be incorporated into the next annual revision of the notice.

The General Services Administration (Office of the Federal Register) will issue more detailed guidance on the formats to be used by agencies in publishing their public notices. The formats prescribed by GSA are to be used to facilitate the annual compilation of the notices and to assure that notices are produced in a consistent manner to make them more useful to the public.

DESCRIBING THE NAME AND LOCATION OF THE SYSTEM IN THE PUBLIC NOTICE

Subsection (e)(4)(A) "The name and location of the system"

Agencies will specify each city/town and site at which the system of records is located. For a geographically dispersed system each location should be listed. A change in the list of locations will not require publication of a revised notice.

While the House report language cited above clearly indicated that the location of each site at which the system is maintained is to be listed, exceptional situations may dictate not including the listing in the body of the notice; e.g., military personnel records which are kept at several hundred installations or certain farmer records which are kept at several thousand county extension agent offices. To include the list of locations in each applicable notice would only serve to inflate the size and thereby reduce the readability of the notice. In these instances, it may be appropriate to publish a single list of field stations, or to refer in the notice for all systems at those sites to a list which is generally available.

DESCRIBING CATEGORIES OF INDIVIDUALS IN THE PUBLIC NOTICE

Subsection (e)(4)(B) "The categories of individuals on whom records are maintained in the system;"

"The purpose of this requirement is for an individual to determine if information on him might be in [the] system. The description of the categories should therefore be clearly stated in non-technical terms understandable to individuals unfamiliar with data collection

techniques." (House Report 93-1416, p.15). For example, the notice might indicate that the records are maintained on students who applied for loans under a student loan program, not persons who filed form X or who are eligible under section ABC-000.

Any change which has the effect of adding new categories of individuals on whom records are maintained will require publication of a revised public notice. If, in the absence of a revised notice, an individual who is the subject of a record in the system would not recognize that fact, a revision should be issued before that change is put into effect. A narrowing of the coverage of the system does not require advance issuance of a revised notice.

DESCRIBING CATEGORIES OF RECORDS IN THE PUBLIC NOTICE

> Subsection (e)(4)(C) "The categories of records maintained in the system;"

This portion of the notice should briefly describe the types of information contained in the system; e.g., employment history or earnings records. As with the previous item, non-technical terms should be used. The addition of any new categories of records not within the categories described in the then current public notice will require the issuance of a revised public notice before that change is put into effect. The addition of a new data element clearly within the scope of the categories in the notice would not require the issuance of a revised notice.

DESCRIBING ROUTINE USES IN THE PUBLIC NOTICE

> Subsection (e)(4)(D) "Each routine use of the records contained in the system, including the categories of users and the purpose of such use;"

In describing the "routine uses" of the system in the public notice, the notice should be sufficiently explicit to communicate to a reader unfamiliar with the technical aspects of the system or the agency's program.

For a more extensive discussion of "routine uses", see subsections (a)(7) (definitions), (b)(3) (conditions of disclosure), (e)(3)(C) (notification to the individual), and (e)(11) (notice of routine uses).

Any new use or significant change in an existing use of the system which has the effect of expanding the availability of the information in the system will require publication of a revised public notice. Any such change in a routine use must also be described in a notice in the Federal Register to permit public comment before it is implemented.

DESCRIBING RECORDS MANAGEMENT POLICIES AND PRACTICES IN THE PUBLIC NOTICE

Subsection (e)(4)(E) "The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;"

This portion of the public notice should describe how the records are maintained, how they are safeguarded, what categories of officials within the agency are permitted to have access, and how long records are retained both on the agency's premises and at secondary storage sites.

In describing record "storage", the agency should indicate the medium in which the records are maintained (e.g., file folders, magnetic tape). "Retrievability" covers the capabilities in the system of records to index and access a record (e.g., by name, combinations of personal characteristics, identification numbers). "Access controls" describes, in general terms, what measures have been taken to prevent unauthorized disclosure of records (e.g., physical security, personnel screening) and what categories of individuals within the agency have access. "Retention" and "disposal" cover the rules on how long records are maintained, if and when they are moved to a Federal Records Center or to the Archives, if and how they are destroyed. The description shall not describe security safeguards in such detail as to increase the risk of unauthorized access to the records.

Changes in this item will not normally require immediate publication of a revised public notice unless they reflect an expansion in the availability of or access to the system of records.

IDENTIFYING OFFICIAL(S) RESPONSIBLE FOR THE SYSTEM IN THE PUBLIC NOTICE

Subsection (e)(4)(F) "The title and business address of the agency official who is responsible for the system of records;"

This portion of the notice must include the title and address of the agency official who is responsible for the policies and practices governing the system described in (e)(4)(E), above. For geographically dispersed systems, where individuals must deal directly with agency officials at each location in order to exercise their rights under the Act (e.g., to gain access), the title and address of the responsible official at each location should be listed in addition to the agency official responsible for the entire system. See discussion of subsection (e)(4)(A), above, for special treatment of certain multiple location systems.

A revised public notice shall be issued before the implementation of any change in the address to which individuals may present themselves in person to inquire whether they are the subject of a record in the system or to seek access to a record or in the address to which individuals may mail inquiries, unless the agency has established internal procedures to assure that mail will be forwarded promptly so that the agency will be able to respond to inquiries within the time constraints established in subsection (d). Generally, changes of this type in the interim between the annual publications of the compilation of notices should be avoided if at all possible. Individuals are more

likely to rely upon the annual compilation and are not as likely to be aware of modifications publicized only by means of separate notice in the Federal Register.

DESCRIBING PROCEDURES FOR DETERMINING IF A SYSTEM CONTAINS A RECORD ON AN INDIVIDUAL IN THE PUBLIC NOTICE

> Subsection (e)(4)(G) "The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;"

This portion of the notice should specify as a minimum, the following:

- The address of the agency office to which inquiries should be addressed or addresses of the location(s) at which the individual may present a request in person. Wherever practicable, this list should be the same as the list of officials responsible for the system in subsection (e)(4)(F), above. If this is the case, it need not be reported.

- What identifying information is required to as certain whether or not the system contains a record about the inquirer.

The agency may require proof of identity only where it has made a determination that knowledge of the fact that a record about an individual exists would not be required to be disclosed to a member of the public under section 552 of title 5 of the United States Code (the Freedom of Information Act). For example, an agency may determine that disclosure of a record in a file pertaining to conflicts of interests would be a clearly unwarranted invasion of personal privacy, within the meaning of 5 USC 552(b)(6), and in this instance the agency may require proof of identity.

A revised public notice will be issued before effecting any change which meets the criteria outlined in subsection (e)(4)(F), above.

This portion of the notice must be consistent with agency rules promulgated pursuant to subsection (f)(1). Any change in these procedures is subject to the requirements of the Administrative Procedure Act as specified in subsection (f).

DESCRIBING PROCEDURES FOR GAINING ACCESS IN THE PUBLIC NOTICE

> Subsection (e)(4)(H) "The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and"

This portion of the public notice must include the mailing address(es) and, if possible, the telephone number(s) of official(s) who can provide assistance; and the location of offices to which the individual may go to seek information.

This provision does not specifically require that the actual procedures for obtaining access or for contesting the accuracy of a record be included in the public notice. It only requires that individuals be advised of the means by which they can obtain information on those procedures. However, it should be noted that, pursuant to subsection (f), agencies are required to publish rules which stipulate the procedures whereby the individual can exercise each of these rights and that these rules are required to be incorporated into the annual compilation of notices and rules published by the Office of the Federal Register.

A revised public notice shall be issued before effecting any change about which the individual would have to know in order to exercise his or her rights under the Act. Changes of this type in the interim between the annual publications of the compilation of notices should be avoided if at all possible.

This portion of the notice must be consistent with agency rules promulgated pursuant to subsections (f)(2) and (3). Any change in these procedures is subject to the requirements of the Administrative Procedure Act as specified in subsection(f).

DESCRIBING CATEGORIES OF INFORMATION SOURCES IN THE PUBLIC NOTICE

Subsection (e)(4)(I) "The categories of sources of records in the system;"

For systems of records which contain information obtained from sources other than the individual to whom the records pertain, the notice should list the types of sources used; e.g.,

- previous employers,
- financial institutions,
- educational institutions attended, or
- peer reviewers (such as in connection with records of the review of proposals for reseach projects)

The notice should indicate if the individual to whom the records pertain is a source of the information in the record. Otherwise all the notices will appear to be violating the requirement that individuals be the main source of information pertaining to them.

Specific individuals or institutions need not be identified. Guidance on when the identity of a source may be withheld is contained in subsection (k)(2), (5) and (7).

STANDARDS OF ACCURACY

Subsection (e)(5) "Maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is

reasonably necessary to assure fairness to the individual in the determination;"

The objective of this provision is to minimize, if not eliminate, the risk that an agency will make an adverse determination about an individual on the basis of inaccurate, incomplete, irrelevant, or out-of-date records that it maintains. Since the final determination as to accuracy is necessarily judgmental, it is particularly critical that this judgment be made with an understanding of the intent of the Act.

The Act recognizes the difficulty of establishing absolute standards of data quality by conditioning the requirement with the language "as is reasonably necessary to assure fairness to the individual...." This places the emphasis on assuring the quality of the record in terms of the use of the record in making decisions affecting the rights, benefits, entitlements, or opportunities (including employment) of the individual.

A corollary provision (subsection (e)(6), below) requires that agencies apply the same standard to records which are disclosed, except when they are disclosed to a member of the public under the Freedom of Information Act or to another agency. (An agency would be subject to the Act and, therefore, would have to apply its own standards of accuracy, etc.)

Agencies may develop tolerances for "accuracy" and "timeliness" giving consideration to the likelihood that errors within those tolerances could result in an erroneous decision with adverse consequences to the individual (e.g., denial of rights, benefits, entitlements, or employment). For example, for its purposes in determining entitlements based on income, it may only be necessary for an agency to record the fact that income was greater than or less than a stipulated level rather than to ascertain and record the precise amount. In questionable instances, reverification of pertinent information with the individual to whom it pertains may be appropriate.

Useful criteria for assuring "relevance" and "completeness" may be somewhat more difficult to develop. The pursuit of "completeness" could result in the collection of irrelevant information which, if taken into account in making an agency determination could prejudice the decision. Agencies must limit their records to those elements of information which clearly bear on the determination(s) for which the records are intended to be used, and assure that all elements necessary to the determinations are present before the determination is made.

VALIDATING RECORDS BEFORE DISCLOSURE

Subsection (e)(6) "Prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;"

While the Act recognizes that an agency cannot guarantee the absolute accuracy of its systems of records, any record disclosed to a person outside the agency (except another agency) must be as accurate as appropriate for purposes of the agency which maintained the record. (See subsection (e)(5)). The only exceptions to this requirement are for disclosures to another agency or to the public under the Freedom of Information Act which may not be delayed or impeded.

Recognizing that an agency properly disclosing information (pursuant to subsection (b), conditions of disclosure) is often not in a position to evaluate acceptable tolerances of error for the purposes of the recipient of the information, the primary objective of this provision is, nonetheless, to assure that reasonable efforts are made to assure the quality of records disclosed to persons who are not subject to the provisions of subsection (e)(5). The agency must, therefore, make reasonable efforts to assure that a record it discloses is as accurate, relevant, timely, and complete as would be reasonably necessary to assure fairness in any determination that it might make on the basis of that record. It may, for example, be appropriate to advise recipients that the information disclosed was accurate as of a specific date, such as the last date on which a determination was made by the agency on the basis of the record or of other known limits on its accuracy e.g., its source.

RECORDS ON RELIGIOUS OR POLITICAL ACTIVITIES

> Subsection (e)(7) "Maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;"

Whereas subsection (e)(1) generally enjoins agencies from collecting information not "relevant and necessary to accomplish a purpose of the agency," this provision establishes an even more rigorous standard governing the maintenance of records regarding the exercise of First Amendment rights. These include, but are not limited to religious and political beliefs, freedom of speech and of the press, and freedom of assembly and petition.

In determining whether or not a particular activity constitutes the exercise of a right" guaranteed by the First Amendment", agencies will apply the broadest reasonable interpretation.

Records describing the exercise of these rights may be maintained only if one of the following conditions is met:

- A statute specifically authorizes it. Specific authorization means that a statute explicitly provides that an agency may maintain records on activities whose exercise is covered by the First Amendment; not merely that the agency is authorized to establish a system of records. However, the statute need not address itself specifically to the maintenance of records of First Amendment activities if it specifies that such activities are relevant to a determination concerning the individual. For

example, since the Immigration and Nationality Act makes the possibility of religious or political persecution relevant to a stay of deportation, the information on these subjects may be admitted in evidence, and therefore would not be prohibited by this provision.

- The individual expressly authorizes it; e.g., a member of the armed forces may indicate a religious preference so that, if seriously injured or killed while on duty, the proper clergyman can be called. The individual may also volunteer such information and if he does so, the agency is not precluded from accepting and retaining it. Thus, if an applicant for political appointment should list his political affiliation, association memberships, and religious activities, the agency may retain this as part of his application file or include it in an official biography. Similarly, if an individual volunteers information on civic or religious activities in order to enhance his chances of receiving a benefit, such as executive clemency, the agency may consider information thus volunteered. However, nothing in the request for information should in any way suggest that information on an individual's First Amendment activities is required.

- The record is required by the agency for an authorized law enforcement function.

In the discussions on the floor of the House regarding the authority to maintain such records for law enforcement purposes, it was stated that the objective of the law enforcement qualification on the general prohibition was "to make certain that political and religious activities are not used as a cover for illegal or subversive activities." However, it was agreed that "no file would be kept of persons who are merely exercising their constitutional rights..." and that in accepting this qualification "there was no intention to interfere with First Amendment rights" (Congressional Record, November 20, 1974, H10892 and November 21, 1974, H10952)

NOTIFICATION FOR DISCLOSURES UNDER COMPULSORY LEGAL PROCESS

Subsection (e)(8) "Make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;"

When a record is disclosed under compulsory legal process (e.g., pursuant to subsection (b)(11)), and the issuance of that order or subpoena is made public by the court or agency which issued it, agencies must make reasonable efforts to notify the individual to whom the record pertains. This may be accomplished by notifying the individual by mail at his or her last known address. The most recent address in the agency's records will suffice for this purpose and no separate address records are required. Upon being served with an order to disclose a record, the agency should endeavor to determine whether the issuance of the order is a matter of public record and, if

it is not, seek to be advised when it becomes public. An accounting of the disclosure, pursuant to subsection (c)(1), is also required to be made at the time the agency complies with the order or subpoena.

RULES OF CONDUCT FOR AGENCY PERSONNEL

> Subsection (e)(9) "Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalities for noncompliance;"

Effective compliance with the provisions of this Act will require informed and active support of a broad cross section of agency personnel. It is important that all personnel who in any way have access to systems of records or who are engaged in the development of procedures or systems for handling records, be informed of the requirements of the Act and be adequately trained in agency procedures developed to implement the Act. Personnel with particular concerns include, but are not limited to, those engaged in personnel management, paperwork management (reports, forms, records, and related functions), computer systems development and operations, communications, statistical data collection and analysis, and program evaluation. (The Communications Act of 1934 prescribes standards and penalties for personnel engaged in handling interstate communications and shall also be consulted, where applicable, when agency rules of conduct are being developed).

Activities under this provision will include

- the incorporation of provisions on privacy into agency standards of conduct;

- the discussion of individual employee responsibilties under the Act in general personnel orientation programs; and

- the incorporation of training on the specific procedural requirements of the Act into both formal and informal (on-the-job) training programs.

Concurrently, those agencies with broad policy development and training responsibilities (e.g., the General Services Administration, the Civil Service Commission) will also be revising their programs as appropriate to augment agency activities in this area.

This provision is also important in ensuring that individuals who are potentially criminally liable or whose actions could expose the agency to civil suit (under subsections (i) and (g), respectively) are fully informed of their obligations under the Act.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

> Subsection (e)(10) "Establish appropriate administrative, technical, and physical safeguards to insure the security and

> confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;"

The development of appropriate administrative, technical, and physical safeguards will, necessarily, have to be tailored to the requirements of each system of records and other related requirements for security and confidentiality. The need to assure the integrity of and to prevent unauthorized access to, systems of records will be determined not only by the requirements of this Act but also by other factors like the requirement for continuity of agency operations, the need to protect proprietary data, applicable access restrictions to protect the national security, and the need for accuracy and reliability of agency information.

While the technology of system security (both for computer-based and other systems of records) is well developed as it relates to materials classified for reason of national defense or foreign policy, few standards currently exist to guide the "civil" agency in this area. Until such standards are developed and promulgated, agencies will be required to analyze each system as to the risk of improper disclosure of records and the cost and availability of measures to minimize those risks. The Department of Commerce (National Bureau of Standards) will be issuing guidelines and standards to assist agencies in evaluating various technological approaches to providing security safeguards in their system and for assessing risks.

NOTICE FOR NEW/REVISED ROUTINE USES

> Subsection (e)(11) "At least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency."

Agencies are required to publish in the Federal Register a notice of their intention to establish "routine uses" for each of their systems of records. Although this provision is designed to supplant the informal rule-making provisions of 5 USC 553, the accommodation of the public comments in the judicial review of the rule-making exercise was intended wherever practicable. Agencies should furnish as complete an explanation of the routine uses and any changes made or not made as a result of the public comment as possible so that the public will be fully informed of the proposed use. This is to give the public an opportunity to comment on the appropriateness of those uses before they come into effect. This notice should be published sufficiently in advance of the proposed effective date of the use to permit time for the public to comment and for the agency to review those comments, but in no case may a new "routine use" be used as the basis for a disclosure less than 30 days after the publication of the "routine use" notice in the Federal Register. A revised public notice

(subsection (e)(4)) must be published before a "routine use" is put into effect; i.e., before a record is disclosed for such a use.

It is clearly permissible to publish the entire system notice (prescribed by subsection (e)(4)) as the notice of "routine use" provided that such "routine uses" are not put into effect until the required 30 day notice period. If an entire system notice is not published, the notice of "routine use" issued pursuant to subsection (e)(11) must, as a minimum, contain

- the name of the system of records for which the "routine use" is to be established;
- where feasible, the authority for the system (see discussion of subsection (e)(1), and the required notice to the individual in subsection (e)(3)(A)), above);
- the categories of records maintained;
- the proposed "routine use(s)";
- and the categories of recipients for each proposed "routine use".

For new "routine uses" of systems for which a public notice under subsection (e)(4) has already been published, reference should be made to that public notice.

A notice in the Federal Register inviting public comment on a proposed new "routine use" is required

- for all existing systems of records not later than August 28, 1975. (Since 30 days advance notice of a "routine use" is required, an agency that fails to publish necessary notices for existing systems on or prior to August 28 may find that it is precluded from making necessay interagency transfers until it has complied with this provision);
- for an existing system of records, whenever a new "routine use" is proposed. A new "routine use" is one which involves disclosure of records for a new purpose compatible with the purpose for which the record is maintained or to a new recipient or category of recipients (even if other uses are concurrently curtailed); and
- for any new systems of records for which "routine uses" are contemplated.

63-619 O - 76 - 69

Section (f)

AGENCY RULES

Subsection (f) "In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall--"

Agencies must promulgate rules to implement the provisions of the Act in accordance with the requirements of section 553 of title 5 of the United States Code including publication of the rules in the Federal Register so that interested persons can have an opportunity to comment. A "rule" is defined as "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedures, or practice requirements of agency... "(5 U.S.C. 551(4)). Formal hearings are not required with respect to rules issued under this section. However, formal hearings are not precluded by this section and, in particular instances, agencies may elect to use the formal hearing procedure.

Two distinct objectives must be satisfied by the rules promulgated pursuant to this subsection:

- they must provide the public with sufficient information to understand how an agency is complying with the law; and

- they must provide sufficient information for individuals to exercise their rights under the Act.

Rules promulgated under this subsection differ from notices under subsection (e) in several ways:

- Rules promulgated under this subsection are subject to requirements of section 553 of the Administrative Procedure Act governing the publication of proposed rules for public comment before issuing them as final rules.

- Rules must only be published twice-as notice of rule making and when they are promulgated as final rules-unless they are subsequently modified. (They will, however, be included in an annual compilation published by GSA.)

- A separate set of rules need not be published for each system of records that an agency maintains. The development of a single set of agency rules is encouraged wherever appropriate.

Agencies are required to publish proposed rules under this subsection allowing at least 30 days for public comment prior to publishing them as final rules. (For systems which will be in use on September 27, 1975, agencies will have to publish rules not later than August 28, 1975.) No further republication of agency rules is required (other

then their inclusion in the annual compilation published by the office of the Federal Register) unless a change is proposed.

The language of subsection (f) explicitly requires "general notice;" i.e., section 553 (b) of title 5 which permits agencies not to publish a general notice if "persons subject thereto are named and either personally served or otherwise have actual notice...." shall not apply to rules promulgated under this subsection. Agencies should also be aware of the fact that, although the presumption is of the validity of the proposed rule, judicial review under the Administrative Procedure Act will be available to assure against arbitrary or capricious actions.

RULES FOR DETERMINING IF AN INDIVIDUAL IS THE SUBJECT OF A RECORD

> Subsection (f)(1) "Establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;"

The procedures for individuals to determine if a system of records contains records pertaining to them should be kept as simple as possible. The published procedures should specify -

- to whom the request should be directed. As discussed above (subsection (e)(4)), for geographically decentralized systems, the individual should not be required to query each location unless the individual can reasonably be expected to be able to discern which location would have a record if one existed; e.g., by place of birth, place of employment. While the development of central indexes to satisfy the requirements of this provision is discouraged, such indexes may be necessary in some instances.

- the information necessary to identify the record. Where the system employs a specialized identification scheme, the individual should not be required to provide such a number or symbol as an absolute requirement, although the individual might be requested to supply it if he or she can reasonably be expected to know it. Instead, alternative combinations of personal characteristics may be used to identify individuals who may have lost, forgotten, or are unaware of their identification numbers or symbols. For example, the combination of name, date of birth, place of birth, and father's first name may be sufficient to identify an individual without the use of a system identification number. As was suggested above, the development of new retrieval and indexing capabilities is not encouraged, rather agencies should exploit existing capabilities to serve individual needs. Restrictions on the use of the Social Security Number as an identifier established by Section 7 of this Act should also be noted where applicable.

- any requirements for verification of identity. These may only be imposed when the fact of the existence of a record would not be required to be disclosed under the Freedom of Information Act (5. U.S.C. 552).

Agency procedures should provide for acknowledgement of the inquiry within 10 days (excluding Saturdays, Sundays, and legal public holidays).

RULES FOR HANDLING REQUESTS FOR ACCESS

> Subsection (f)(2) "Define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;"

The development of procedures for individuals to identify themselves for the purposes of gaining access to their records will necessarily vary depending on the nature, location, and sensitivity of the records in the system. Care must be exercised to assure that the requirements for verification of identity are not so cumbersome as to prevent individuals from gaining access to records to which they are entitled to have access. The requirements pertaining to verification of identity contained in subsection (f)(1), above, should also be noted.

"Reasonableness" will be measured in terms of

- the risk of access being granted to an individual who is not entitled to access weighed against the probable harm (including embarrassment) to the individual to whom the record pertains which would result from unauthorized access; and

- the standards for verification of identity which a typical individual about whom record is maintained could be expected to meet.

When agencies specify that individuals may (or must) present themselves in person to verify their identity, hours and locations specified should take into account the kinds of individuals about whom records are maintained. For example, it may be appropriate to ask a current employee who seeks access to his record to present himself to the agency personnel office during normal working hours. No requirements may be established which would have the effect of impeding an individual in exercising his or her right to access.

Agencies which maintain systems of records on widely dispersed groups of individuals and which have field offices equipped to do so, are encouraged to use those offices as sites at which an individual can present a request for access even though his or her records may not be maintained at any one of those field offices. The information necessary to identify individuals should be kept to the absolute minimum and neither this provision nor any other provision of the Act should be used for the purpose of acquiring and storing additional information about an individual.

The published rules prescribing procedures for verification of identity will include--

- a list of the locations and/or mailing addresses of locations to which the request may be presented;

- when in-person verification is required or permitted, the hours when those locations are open (including the dates of holidays on which they are closed); and

- documents which the agency will require, if any, to establish the identity of the individual (specifying as many alternatives as possible).

RULES FOR GRANTING ACCESS TO RECORDS

Subsection (f)(3) "Establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure [sic], if deemed necessary, for the disclosure to an individual of medical records including psychological records, pertaining to him;

Individuals may be granted access to their records either in person or by having copies mailed to them. The nature of the system and of the individuals on whom records are maintained will determine which method is appropriate. If an agency determines that it can grant access to records only by providing a copy of the record through the mail because it cannot provide "reasonable" means for individuals to have access to their records in person, it may not charge a fee for making the copy.

The issue of access to medical records was the subject of extensive discussion during the development of the Act. As written, the Act provides that individuals have an unqualified right of access to records pertaining to them (with certain exceptions specified in subsections (j) and (k), below) but that the process by which individuals are granted access to medical records may, at the discretion of the agency, be modified to prevent harm to the individual. [See subsection (d)(1).]

As a minimum, rules issued pursuant to this subsection shall be consistent with the requirements of subsection (d)(1) and should include--

- some indication, for requests presented in person, as to whether the individual can expect to be granted immediate access to the record and, for written request, the expected time lag, if any, between receipt of a request for access and the granting of that access (see subsection (d)(2) for guidance on maximum response times); and

- the locations at which individuals will be granted access to their records or the fact that access will be granted by providing copies by mail;

- notice that an individual when reviewing a record in person, may be accompanied by another individual of his or her choosing and the agency's requirements, if any, for a written statement

authorizing that individual's presence. Such authorization statements, if employed, should be as brief as possible.

RULES FOR AMENDING RECORDS

Subsection (f)(4) "Establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section;"

Agency procedures for permitting an individual to request amendment of a record shall be consistent with subsections (d)(2) and (3) and shall as a minimum, specify--

- the official(s) to whom the request is to be directed;
- the identifying information required to relate the request to the appropriate record;
- the official(s) to whom a request for a review of an initial adverse determination on request to amend may be taken; and
- offices/officials from whom assistance can be obtained in preparing a request to amend a record or to appeal an initial adverse determination or to learn further of the provisions for judicial review.

If the agency deems it appropriate to establish (or already has) a formal reviewing mechanism for assessing the accuracy of its records or for reconciling disputes, that mechanism or board should be described in its rules published pursuant to this subsection. This provision does not require the establishment of new, separate review mechanisms where such capabilities exist and are, or can be modified to be, in conformance with this Act.

RULES REGARDING FEES

Subsection (f)(5) "Establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record."

Fees may be charged to an individual under this section only for the making of copies of records when requested by the individual. As stated above (subsection (f)(3)), when copies are made by the agency incident to granting access to a record, a fee may not be charged. (It should be noted that the provisions on fees charged to an individual under this Act differ from those governing fees charged to the public. See 5 U.S.C 552, as amended, the Freedom of Information Act, for guidance on fees for copies of records made available to the public.)

"[An]agency may not charge the individual for time spent searching for requested records or for time spent in reviewing records to determine if they fall within the disclosure requirements of the Act." (House Report 93-1416, p.17) When an individual requests a copy of a record, pursuant to subsection (d)(1) (access to records), the fee charged may not exceed the direct cost of making the copy (printing, typing, or photocopying and related personnel and equipment costs) and may not include any cost of retrieving the information. In establishing fee schedules, agencies should also consider the cost of collecting the fee in determining when fees are appropriate.

ANNUAL PUBLICATION OF NOTICES AND RULES

> Subsection (f)(final paragraph - unnumbered) "The Office of the Federal Register shall annually compile and publish the rules promulgated under this section and agency notices published under section (e)(4) of this section in a form available to the public at low cost"

The annual compilation of public notices (subsection (e)(4)) and agency rules (subsection (f)(1) through (5)) will be produced in a form which promotes the exercise of individual rights under this Act.

The General Services Administration will issue guidance on the format and timing for submission of rules and notices to reduce the cost of preparing and publishing the rules and notices, to minimize redundancy wherever possible, and otherwise to enhance the utility of these publications. For example, the various provisions of subsection (e)(4) and (f)(1) through (4) calling for lists of names and addresses need not be treated as separate portions of the annual notice for each system.

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (g)

CIVIL REMEDIES

This subsection prescribes the circumstances under which an individual may seek court relief in the event that a Federal agency violates any requirement of the Privacy Act or any rule or regulation promulgated thereunder, the basis for judicial intervention, and the remedies which the courts may prescribe. It should be noted that an individual may have grounds for action under other provisions of the law in addition to those provided in this section. For example -

- An individual may seek judicial review under other provisions of the Administrative Procedure Act (APA).

- An individual may file a complaint alleging possible criminal misconduct under section (i), below.

- A Federal employee may file a grievance under personnel procedures. It should also be noted that an agency/employee responsible for an adverse action against an individual may be personally subject to civil suit, particularly where the agency/employee acted in a manner that was intentional or willful.

Judgments, costs, and attorney's fees assessed against the United States under this subsection would appear to be payable from the public funds rather than agency funds. 28 U.S.C. 2414 and 31 U.S.C. 724a (Payment of Judgements); 28 U.S.C. 1924 (Costs). While it is not the purpose of these guidelines to discuss the jurisdiction of the district courts or the procedures in such cases, it should be noted that most cases arising under subsection (g) will be handled by the General Litigation Section of the Civil Division of the Department of Justice. In these cases, upon receipt of a copy of the summons and complaint served upon the Attorney General and notification of its filing by the United States Attorney (see Rule 4, Federal Rules of Civil Procedure), the General Litigation Section will request the agency to furnish a litigation report.

Some agencies are authorized to conduct their own litigation. Where its authority permits, the agency may decide to handle its own cases under this Act. In view of the general litigation responsibility which the Department of Justice has for all other departments and agencies in the executive branch, it is important that agencies handling their own litigation under this Act keep the Department of Justice currently informed of their progress, and forward to the Civil Division copies of significant documents which are filed in such cases.

Each agency should maintain a complete and careful record of the administrative procedures followed in processing this statute. The record should be maintained so that it can be readily certified as the complete administrative record of the proceedings as a basis for possible use in litigation.

GROUNDS FOR ACTION Subsection (g)(1) "Civil Remedies. Whenever any agency"

The subsection authorizing civil actions by individuals is designed to assure that an individual who (1) was unsuccessful in an attempt to have an agency amend his or her record; (2) was improperly denied access to his or her record or to information about him or her in a record; (3) was adversely affected by an agency action based upon an improperly constituted record; or (4) was otherwise injured by an agency action in violation of the Act will have a remedy in the Federal District courts.

REFUSAL TO AMEND A RECORD

Subsection (g)(1)(A) "Makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;"

An individual may seek judicial review of an agency's determination not to amend a record pursuant to a request filed under subsection (d)(2) under either one of two conditions--

- the individual has exhausted his or her recourse under the procedures established by the agency pursuant to subsection (d)(3) (appeals on the agency's refusal to amend) and the reviewing official has also refused to amend the record, or

- the individual contends that the agency has not considered the request to review in a timely manner or otherwise has not acted in a manner consistent with the requirements of subsection (d)(3). Such an action could presumably involve a challenge either to the agency's procedures published under subsection (f)(4) or to the agency head's decision to extend the period of review "for good cause shown" under subsection (d)(3).

An individual may also bring a civil action based on allegedly inaccurate records if it can be shown that a decision adverse to the individual resulted from that inaccuracy. See subsection (g)(1)(C). However, no test of injury is required to bring an action under subsection (g)(1)(A).

The basis for judicial review and the available remedies in actions brought under this subsection are found in subsection (g)(2).

DENIAL OF ACCESS TO A RECORD

Subsection (g)(1)(B) "Refuses to comply with an individual request under subsection (d)(1) of this section;"

Under this subsection, individuals may challenge a decision to deny them access to records to which they consider themselves entitled (under subsection (d)(1)). The action giving rise to the suit may be the agency head's determination (pursuant to subsection (k), specific exemptions) to exempt a system of records from the requirements that individuals be granted access. "Since access to a file is the key to insuring the citizen's right of accuracy, completeness, and relevancy, a denial of access affords the citizen the right to raise these issues in court. This would be the means by which a citizen could challenge any exemption from the requirements of [the Act]." (Senate Report 93-1183, p. 82). It should be noted that systems of records covered under subsection (j) (general exemptions) are permitted to be exempted from this provision.

This provision is also the one by which individuals may contest an agency's refusal to grant access as a result of its interpretation of the definitions in the Act as they apply to information maintained by an agency and for the exclusion set forth in subsection (d)(5), denial of access to records compiled in reasonable anticipation' of litigation. No test of injury is required to bring action under subsection (g)(1)(B). The basis for judicial review and available remedies are found in subsection (g)(3).

FAILURE TO MAINTAIN A RECORD ACCURATELY,

> Subsection (g)(1)(C) "Fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities, of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or"

An individual may bring an action under this subsection only if it can be shown that the deficiency in the record resulted in an adverse determination by the agency which maintained the record, on the basis of the record. "An action also lies if the agency makes an adverse determination based upon a record which is inaccurate, untimely, or incomplete. However, in order to sustain such action, the individual must demonstrate the causal relationship between the adverse determination and the incompleteness, inaccuracy, irrelevance or untimeliness of the record." (House Report 93-1416, p. 17)

An adverse action is one resulting in the denial of a right, benefit, entitlement, or employment by an agency which the individual could reasonably have been expected to have been given if the record had not been deficient. This provision, in essence, allows an individual to test the agency's compliance with subsection (e)(5).

It should also be noted that, under this subsection, an agency may be liable as a consequence of its failure to maintain a record accurately only if it is shown that its failure has been "intentional or willful" (subsection (g)(4)). (No such test is required under the provisions of

subsection (g)(1)(A), above, under which an individual can seek a review of the accuracy of a record)

Neither this subsection nor subsection (g)(1)(A) was intended to permit an individual collaterally to attack information in records pertaining to him which has already been the subject of or for which adequate judicial review is available. For example, these provisions were not designed to afford an individual an alternate forum in which he can challenge the basis for a criminal conviction or an asserted tax deficiency.

The basis for judicial review and available remedies are found in subsection (g)(4).

OTHER FAILURES TO COMPLY WITH THE ACT

> Subsection (g)(1)(D) "Fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,"

In addition to the grounds specified in subsections (g) (1) (A) through (C) above, an individual may bring an action for any other alleged failure by an agency to comply with the requirements of the Act or failure to comply with any rule published by the agency to implement the Act (subsection (f)) provided it can be shown that--

- the action was "intentional or willful";

- the agency's action had an "adverse effect" upon the individual; and

- the "adverse effect" was causally related to the agency's actions.

The basis for judicial review and available remedies provided by this Act are found in subsection (g)(4).

BASIS FOR JUDICIAL REVIEW AND REMEDIES FOR REFUSAL TO AMEND A RECORD

> Subsection (g)(2)"(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.
>
> "(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed."

When an individual seeks judicial review of the accuracy, timeliness, completeness, or relevance of a record either as a result of a challenge to the agency's refusal to amend a record or because the

individual alleges that the agency's process for review does not conform to subsection (d)(3), the court is required to review the matter as if it were an initial determination (de novo). Such a review may extend to the agency's criteria established in conformance with subsections (e)(1) and (5) for "accuracy, relevance, timeliness, and completeness" as they relate to the purposes for which the agency maintains the record.

Unlike the judicial review of a denial of access to a record, in a review of refusal to amend a record the burden to justify its action is not expressly placed upon the agency by the Privacy Act. This was intended to result in placing the burden of challenging the accuracy of the record upon the individual. As a result, agencies should not maintain additional records solely for the purpose of validating the accuracy, timeliness, and completeness or relevence of other records they maintain.

If the court finds for the individual against the agency it may

- direct the agency to amend the record or to take such other steps as it deems appropriate.

- require the agency to pay court costs and attorney fees. "It is intended that such award of fees not be automatic, but rather, that the courts consider the criteria as delineated in the existing body of law governing the award of fees." (House Report 93-1416, p. 17)

BASIS FOR JUDICIAL REVIEW AND REMEDIES FOR DENIAL OF ACCESS

Subsection (g)(3)"(A) In any suit brought under the provision (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

"(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed."

In conducting its review, "[t]he court is required to determine such matters de novo[sic] and the burden of proof is upon the agency to sustain the exemption." (House Report 93-1416, p. 17) In view of the

sensitivity of some of the records to which access may be sought, the court, in examining those records may do so in camera. "A person seeking access to a file which he has reason to believe is being maintained on him for the purposes of determining its accuracy and completeness, for example, or to take advantage of the rights afforded him . . . . could raise the question of the propriety of the exemption which denies him access to his files. In deciding whether the citizen has a right to see his file or to learn whether the agency has a file on him, the court would of necessity have to decide the legitimacy of the agency's reasons for the denial of access, or refusal of an answer. The Committee intends that any citizen who is denied a right of access under the Act may have a cause of action, without the necessity of having to show that a decision has been made on the basis of it, and without having to show some further injury, such as loss of job or other benefit, that might stem from the denial of access." (Senate Report 93-1183, p. 82). If the court finds for the individual against the agency, it may--

- direct the agency to grant the individual access as provided under subsection (d)(1), above.

- require the agency to pay court costs and attorney fees. "It is intended that such award of fees not be automatic, but rather, that the courts consider the criteria as delineated in the existing body of law governing the award of fees." (House Report 93-1416, p. 17)

BASIS FOR JUDICIAL REVIEW AND REMEDIES FOR ADVERSE DETERMINATION AND OTHER FAILURES TO COMPLY

Subsection (g)(4) "In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--

"(A) Actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

"(B) The costs of the action together with reasonable attorney fees as determined by the court."

In any action brought for failure to comply with the provisions of the Act, other than those covered in subsection (g) (1) (A) and (B) (refusal to amend a record or denial of access) it must be shown that--

- the failure or the agency to comply was "intentional or willful;"

- there was injury or harm to the individual; and

- the injury was causally related to the alleged agency failure.

As indicated above, these criteria do not apply to suits brought to amend a record pursuant to subsection (g) (1) (A) so that an individual may, under certain circumstances, properly bring an action either under subsections (g) (1) (A) or (g) (1) (C).

When the court finds that an agency has acted willfully or intentionally in violation of the Act in such a manner as to have an adverse effect upon the individual, the United States will be required to pay

- actual damages or $1,000, whichever is greater

- court costs and attorney fees.

Unlike subsections (g) (2) and (3) above, which make the award of court costs and attorney fees discretionary in successful suits brought under subsections (g) (1) (A) and (B), such awards are required to be made in actions in which the individual has prevailed under subsections (g) (1) (C) and (D). See House Report 93-1416, pp. 17-18 and the Congressional Record, December 18, 1974, P.H.122445 for further discussion of this point.

JURISDICTION AND TIME LIMITS

> Subsection (g) (5) "An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section."

Action may be brought in the district court for the jurisdiction in which the individual resides, or has a place of business, or in which the agency records are situated, or in the District of Columbia.

"The statute of limitations is two years from the date upon which the cause of action arises, except for cases in which the agency has materially or willfully misrepresented any information required to be disclosed and when such misrepresentation is material to the liability of the agency. In such cases the statute of limitations is two years from the date of discovery by the individual of the misrepresentation." (House Report 93-1416, p. 18)

A suit may not be brought on the basis of injury which may have occurred as a result of an agency's disclosure of a record prior to September 27, 1975; e.g., disclosure without the consent of the individual or an adverse action resulting from a disclosure. This language is intended to preclude agencies from being held liable, under this law, for actions taken prior to its effective date.

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (h)

RIGHTS OF LEGAL GUARDIANS

Subsection (h) "For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual."

This section is intended to ensure that minors or individuals who have been declared to be legally incompetent have a means of exercising their rights under the Act. It also has the effect of making individuals acting in loco parentis to minors, parents, legal guardians, and custodians the same as the individual for purposes of giving consent for disclosure (subsection (b)) and being informed of the purposes for which records are maintained (subsection (e)(3)).

It should be noted that this provision is discretionary and that individuals who are minors are authorized to exercise the rights given to them by the Privacy Act or, in the alternative, their parents or those acting in loco parentis may exerise them in their behalf.

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (i)

CRIMINAL PENALTIES

This subsection establishes criminal sanctions for three possible violations
- Unauthorized disclosure.
- Failure to publish a public notice or a system of records subject to the Act.
- Obtaining access to records under false pretenses.

The first two are directed at actions of officers and employees of Federal agencies and (pursuant to subsection (m)) certain contractor personnel. Agencies should ensure that all personnel are informed of the requirements of the Act and, pursuant to subsection (e)(9), rules of conduct, are given periodic training in this area.

CRIMINAL PENALTIES FOR UNAUTHORIZED DISCLOSURE

> Subsection (i)(1) "Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000."

It is a criminal violation of the provisions of the Act if an employee, knowing that disclosure is prohibited, willfully discloses a record without the written consent of the individual to whom it pertains, at his or her request, or for one of the reasons set forth in subsections (b)(1) through (11), conditions of disclosure.

CRIMINAL PENALTIES FOR FAILURE TO PUBLISH A PUBLIC NOTICE

> Subsection (i)(2) "Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000."

As was discussed in connection with subsection (e)(4), above, a basic objective of the Act is to assure that there is no system of records whose very existence is kept secret. An agency is required to publish a public notice about each system of records which it maintains. It is a criminal violation of the Act willfully to maintain a system of records and not to publish the prescribed public notice. The exemption provisions, subsections (j) and (k), do not allow an

63-619 O - 76 - 70

agency head to exempt any system of records from the requirement to publish a public notice of its existence, although that notice may be somewhat abbreviated. (See subsections (a)(5), definitions, and (e)(4), public notice, for guidelines on what constitutes a system.) It should be noted that, under agency procedures, the officer or employee who maintains the system may not be the one who is responsible for publishing the notice. Agency procedures should make the responsibilities of each clear. The officer or employee who maintains the system has an obligation to notify the one responsible for publishing the notice. Similarly the officer or employee responsible for publishing the notice, once notified of the existence of a system, must make that fact public.

CRIMINAL PENALTIES FOR OBTAINING RECORDS UNDER FALSE PRETENSES

> Subsection (i)(3) "Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000."

This provision makes it a criminal act knowingly and willfully to request or gain access to a record about an individual under false pretenses. It is likely that the principal application of this provision will be to deter individuals from making fraudulent requests under subsection (d)(1), access to records.

Subsections (j) and (k)

EXEMPTIONS

The drafters of the Act recognized that the application of all of the requirements of the Act to certain categories of records would have had undesirable and often unacceptable effects upon agencies in the conduct of necessary public business.

Two categories of exemptions are established: general exemptions (subsection (j)) and specific exemptions (subsection (k)). The principal difference between the two categories is that systems of records exempted under subsection (j) may be exempted from more provisions of the Act than those exempted under subsection (k). Exemptions under subsection (j) may be exempted from the civil remedies provision and, in particular, the judicial review under subsections (g)(1)(B) and (g)(3), civil remedies.

In applying any of the exemption provisions of the Act, it is important to recognize the following:

- No system of records is automatically exempt from any provision of the Act. To obtain an exemption for a system from any requirement of the Act, the head of the agency that maintains the system must make a determination that the system falls within one of the categories of systems which are permitted to be exempted, and publish the determination as a rule in accordance with the requirements (including general notice) of section 553 of the Administrative Procedure Act. That notice must include the specific provisions from which the system is proposed to be exempted and why the agency considers the exemption necessary.

- The requirement to publish a public notice (subsection (e)(4), above) applies to all systems of records maintained by an agency. Certain other provisions such as conditions of disclosure (b), accounting for disclosures((c)(1) and (2)) and restrictions on maintaining records on First Amendment activities ((e)(7)) also apply to all systems of records. Agencies may not exempt any system, as defined in subsection (a)(5) from any of these requirements.

In some instances, systems may contain records which are subject to exemption under more than one subsection in subsections (j) or (k). In those cases the notices claiming exemption should, if possible, specify which types of records are subject to which exemption.

Agency records which are part of an exempted system may be disseminated to other agencies and incorporated into their non-exempt records systems. The public policy which dictates the need for exempting records from some of the provisions of the Act is based on the need to protect the contents of the records in the system -- not

the location of the records. Consequently, in responding to a request for access where documents of another agency are involved, the agency receiving the request should consult the originating agency to determine if the records in question have been exempted from particular provisions of the Act. A copy of the request may be forwarded to the originating agency for handling of its documents where such a procedure would result in a more rapid response to the request for access but the agency receiving the request remains responsible for assuring a prompt response.

Agencies which elect to invoke exemptions are encouraged to adopt procedures similar to those prescribed by the Act wherever appropriate. For example, it may be appropriate to seek an exemption from the access provision ((d)(1)) for certain prisoner records because they contain court controlled pre-sentence reports, but a more limited access procedure may be appropriate.

Subsection (j)

GENERAL EXEMPTIONS
APPLICABILITY AND NOTICE REQUIREMENTS

Subsection (j) "The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553 (b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6),(7), (9), (10), and (11), and (i) if the system of records is--

"(1) . . .

"(2) . . .

"At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section."

This section permits agency heads to exempt systems of records which are maintained by the Central Intelligence Agency or for criminal law enforcement purposes, as further discussed in subsections (j)(1) and (2), below, from all provisions of the Act except!mloe the--

!msingle - conditions of disclosure, ((b));

- accounting for disclosures and retention of the accounting, ((c)(1) and (2));
- annual public notice except for procedures for identifying a record, gaining access to it, contesting its accuracy, and identifying the sources of records, ((e)(4)(A) through (F));
- obligation to check the accuracy, relevance, timeliness, and completeness of records before disclosing them to a person other than another agency or to the public under the Freedom of Information Act, (e)(6));
- restrictions on maintaining records on First Amendment activities, ((e)(7));
- establishment of rules of conduct and administrative, technical, and physical safeguards, ((e)(9) and (10), respectively);
- publication of "routine use" notices ((e)(11)); and
- criminal penalties, ((i)).

When the head of an agency determines that a system of records maintained by the agency should be exempted from certain provisions of the Act, a notice must be published in the Federal Register which specifies, as a minimum:

- the name of the system (This should be the same as that given in the annual public notice under subsection (e)(4)); and
- the specific provisions of the Act from which the system is to be exempted and the reasons therefor. A separate reason need not be stated for each provision from which the system is being exempted, where a single explanation will serve to explain the entire exemption.

The agency head's determination is considered to be a rule under the Administrative Procedure Act (APA) and is subject to the requirements of general notice and public comment of that Act, 5 U.S.C. 553. While general notice of a proposed rule is not required under the APA when "persons subject thereto are named and either personally served or otherwise have actual notice thereof...;" the use of the phrase "including general notice" means that individual notifications will not suffice.

The systems of records and the number of records (i.e., individuals) in each, which were exempted from any of the provisions of the Act under this subsection will be required to be included in the annual report prepared as required by subsection (p). It should be emphasized that the exemption provisions are permissive; i.e., an agency head is authorized, but not required, to exempt a system from all or any portion of selected provisions of the Act when he or she deems it to be in the best interest of the government and consistent with the Act and these guidelines. In commenting on this provision, the House Committee noted:

> "The Committee also wishes to stress that this section is not intended to require the C.I.A. and criminal justice agencies to withhold all their personal records from the individuals to whom they pertain. We urge those agencies to keep open whatever files are presently open and to make available in the future whatever files can be made available without clearly infringing on the ability of the agencies to fulfill their missions." (House Report 93-1416, p. 19)

To the extent practicable, records permitted to be exempted from the Act should be separated from those which are not. Further, while the language permits agency heads to exempt systems of records, agencies should exempt only portions of systems wherever it is possible.

GENERAL EXEMPTION FOR THE CENTRAL INTELLIGENCE AGENCY Subsection (j)(1) "Maintained by the Central Intelligence Agency; or"

GENERAL EXEMPTION FOR CRIMINAL LAW ENFORCEMENT RECORDS

Subsection (j)(2) "Maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision."

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (k)

SPECIFIC EXEMPTIONS

APPLICABILITY AND NOTICE REQUIREMENTS

Subsection (k) "The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1),(2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3),(d),(e)(1), (e)(4)(G),(H), and (I) and (f) of this section if the system of records is--"

"(1)

.

.

.

"(7)...

"At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section."

This subsection permits agency heads to exempt systems of records from a limited number of provisions of the Act. In addition to the provisions from which no system may be exempted under subsection (j), a system which falls under any one of the seven categories listed in this subsection may not be exempted from the following provisions:

- informing prior recipients of corrected or disputed records, ((c)(4));
- collecting information to be used in determinations about an individual directly from the individual to whom it pertains; ((e)(2));
- informing individuals asked to supply information of the authority by and purposes for which it is collected and whether or not providing the information is mandatory, ((e)(3));
- maintaining records with such accuracy, completeness, timeliness, and relevance as is reasonable for the agency's purposes, ((e)(5));
- notifying the subjects of records disclosed under compulsory process, ((e)(8)); and

- civil remedies, (g).

As with subsection (j), upon determining that a system is to be exempted under this section, the agency head is required to publish that determination as a rule under the Administrative Procedure Act subject to public comment. That notice must, as a minimum, specify

- the name of the system (as in the annual notice under subsection ((e)(4)); and

- the specific provisions of the Act from which the system is to be exempted and the reason therefor.

The agency head's determination is considered to be a rule under the Administrative Procedure Act (APA) and is subject to the requirements of general notice and public comment of that Act, 5 U.S.C. 553. While general notice of a proposed rule is not required under the APA when "persons subject thereto are named and either personally served or otherwise have actual notice thereof...", the language "including general notice" means that individual notification will not suffice.

In addition, the systems of records and the number of records in each, which were exempted from any of the provisions or the Act under this section will be required to be included in the annual report required by subsection (p).

It should also be noted that the exemption provisions are permissive; i.e., an agency head is authorized, but not required, to exempt a system when he or she deems it to be in the best interest of the government and consistent with the Act and these guidelines. "Also as with section (j) records, the Committee urges agencies maintaining section (k) records to open those documents to the individuals named in them insofar as such action would not impair the proper functioning of those agencies." (House Report 93-1416, p. 20)

In the process of utilizing any of these exemptions, agencies should, wherever practicable, segregate those portions of systems for which an exemption is considered necessary so as to hold to the minimum the amount of material which is exempted. While the language permits agency heads to exempt entire systems of records, the language of certain of the specific provisions below suggests that it may, in some instances, be appropriate to exempt only portions of systems where it is not possible to segregate entire systems. For example, records containing classified material to which access may be denied under (k)(1) should be screened to permit access to unclassified material, and only these portions of investigative material which meet all of the criteria in (k)(2) or (5) should be withheld. However, in the case of records which are permitted to be exempted to the extent that their disclosure would reveal the identity of a confidential source, extreme care should be exercised to ensure that the content of any records being segregated does not disclose the identity of the source.

EXEMPTION FOR CLASSIFIED MATERIAL

Subsection (k)(1) "Subject to the provisions of section 552(b)(1) of this title;"

This subsection permits agency heads to exempt, from certain provisions of the Act, those systems of records which are "(A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order." (5 U.S.C. 552(b)(1), as amended by Public Law 93-502)

The Freedom of Information Act, as amended by P.L. 93-502, authorizes de novo judicial review of an agency's decision to classify a document, including in camera examination of the document when the court deems it necessary to resolve a dispute as to whether a document is properly being withheld under the provisions of subsection (b)(1) of the Freedom of Information Act. See the Conference Report on H.R. 12471, House Report 93-1380, pp 8-9.

Useful guidance in the application of this provision is found in the Senate Committee report discussion of a similar provision on classified materials::

> "The potential for serious damage to the national defense or foreign policy could arise if the notice describing any information system included categories or sources of information... or provided individuals access to files maintained about them...
>
> "The Committee does not by this legislation intend to jeopardize the collection of intelligence information related to national defense or foreign policy, or open to inspection information classified pursuant to Executive Order 11652 to persons who do not have an appropriate security clearance or need to know.
>
> "This section is not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information. Many personnel files and other systems may not be subject to security classification or may not cause damage to the national defense or foreign policy simply by permitting the subjects of such files to inspect them and seek changes in their contents under this Act." (Senate Report 93-1183, p. 74)

EXEMPTION FOR INVESTIGATORY MATERIAL COMPILED FOR LAW ENFORCEMENT PURPOSES

Subsection (k)(2) "Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such

material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;"

This provision allows agency heads to exempt a system of records compiled in the course of an investigation of an alleged or suspected violation of civil laws, including violations of the Uniform Code of Military Justice and associated regulations, except to the extent that the system is more broadly exempt under the provision covering records maintained by an agency whose principal function pertains to the enforcement of criminal laws (subsection (j)(2)). This exemption was drafted because "[i]ndividual access to certain law enforcement files could impair investigations, particularly those which involve complex and continuing patterns of behavior. It would alert subjects of investigations that their activities are being scrutinized, and thus allow them time to take measures to prevent detection of illegal action or escape prosecution." (House Report 93-11416, p. 19)

The phrase "investigatory material compiled for law enforcement purposes" is the same phrase as opened exemption (b)(7) to the Freedom of Information Act prior to its recent amendment (Public Law 93-502), with the exception of the use of the word "material" in the Privacy Act for the word "files" in the now amended Freedom of Information Act exemption. The intent was to have the same meaning given to this phrase in the Privacy Act as had been given to it in the Freedom of Information Act except that the phrase would apply to material as opposed to entire files. The case law, then, which had interpreted "investigatory" and "compiled" and "law enforcement purposes" for the now amended portions of exemption (b)(7) of the Freedom of Information Act should be utilized in defining those terms as they appear in subsection (k)(2) of the Privacy Act.

It was further recognized that "due process" in both civil action and criminal prosecution will assure that individuals have a reasonable opportunity to learn of the existence of, and to challenge, investigatory records which are to be used in legal proceedings.

To the extent that such an investigatory record is used as a basis for denying an individual any right, privilege, or benefit (including employment) to which the individual would be entitled in the absence of that record, the individual must be granted access to that record except to the extent that access would reveal the identity of a confidential source.

The language permitting an agency to withhold records used as a basis for denying a benefit to the extent that the record would reveal the identity of an individual who furnished information in confidence is very narrowly drawn and must be treated carefully (see also subsections (k)(5) and (7), below). For information collected on or subsequent to the effective date of this section (September 27, 1975) a record may only be withheld to protect the identity of a source if

- an express guarantee was made to the source that his or her identity would not be revealed. (Such guarantees should be made on a selective basis; i.e., individuals from whom information is solicited for law enforcement purposes should be advised that their identity may be disclosed to the individual to whom the record pertains unless a source expressly requests that his or her identity not be revealed as a condition of furnishing the information.); and

- the record, if stripped of the identity of the source would nonetheless by its content reveal the identity to the subject.

It was recognized that the type of investigatory record covered by subsection (k)(2) currently contains substantial information which was obtained with the tacit understanding that the identity of the source would not be revealed. For this reason the Act provides that information in such records that was collected prior to the effective date of the Act may be withheld from the individual to whom it pertains to the extent that it was collected under an implied promise that its source would not be revealed and disclosing it would reveal the identity of the source.

The phrase "to the extent that" is particularly important. As implied above, if a record can be disclosed in such a way as to conceal its source, a promise of confidentiality to the source is not sufficient grounds for withholding it. Obviously, the content of certain records is such that it reveals the identity of the source even if the name of the source or other identifying particulars are removed; e.g., the record contains information that could only have been furnished by one individual known to the subject. Only in those cases, may the substance of the record be withheld to protect the identity of a source and then only to the extent necessary to do so. It is recognized, however that it may in some instances be very difficult for an agency to know whether the content of a record would, in and of itself, reveal its source. Therefore, it may be appropriate in light of the intent underlying this exemption, to exempt a record when any reasonable doubt exists as to whether its disclosure would reveal the identity of a confidential source.

Additional guidance on the circumstances under which an agency may withhold a record on the grounds that its disclosure would reveal the identity of a source who provided information under a pledge of confidentiality is found in Senator Ervin's statement on the compromise bill on the floor of the Senate.

> "The compromise provision for the maintenance of information received from confidential sources represents an acceptance of the House language after receiving an assurance that in no instance would that language deprive an individual from knowing of the existence of any information maintained in a record about him which was received from a 'confidential source.' The agencies would not be able to claim that disclosure of even a small part of a particular item would reveal the identity of a confidential source. The confidential information would have to be characterized in some general way. The fact of the item's

existence and a general characterization of that item would have to be made known to the individual in every case.

"Furthermore, the acceptance of this section in no way precludes an individual from knowing the substance and source of confidential information, should that information be used to deny him a promotion in a government job or access to classified information or some other right, benefit or privilege for which he was entitled to bring legal action when the government wished to base any part of its legal case on that information.

"Finally, it is important to note that the House provision would require that all future promises of confidentiality to sources of information be expressed and not implied promises. Under the authority to prepare guidelines for the administration of this act it is expected that the Office of Management and Budget will work closer with agencies to insure that Federal investigators make sparing use of the ability to make express promises of confidentiality." (Congressional Record, December 17, 1974, p.S21816)

The foregoing discussion with respect to confidentiality of sources is also applicable to the provisions of subsections (k)(5) and (7), below.

EXEMPTION FOR RECORDS MAINTAINED TO PROVIDE PROTECTIVE SERVICES

Subsection (k)(3) "Maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;"

This exemption covers records which are not clearly within the scope of law enforcement records covered under subsection (k)(2) but which are necessary to assuring the safety of individuals protected pursuant to 18 U.S.C. 3056.

It was noted that "access to Secret Service intelligence files on certain individuals would vitiate a critical part of Secret Service work which was specifically recommended by the Warren Commission that investigated the assassination of President Kennedy and funded by Congress." (House Report 93-1416, p. 19)

EXEMPTION FOR STATISTICAL RECORDS

Subsection (k)(4) "Required by statute to be maintained and used solely as statistical records;"

A "statistical record" is defined in subsection (a)(6) as "a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13."

It is the intent of this provision to permit exemptions for those systems of records which by operation of statute cannot be used to make a determination about an individual.

This provision permits an agency head to exempt a system of records which is used only for statistical, research, or program evaluation purposes, and which is not used to make decisions on the rights, benefits, or entitlements of individuals except as permitted by Section 8 of Title 13. The use of the language "required by statute to be maintained ... only" suggests that systems of records which qualify to be exempted under this provision are those composed exclusively of records that by statute are prohibited from being used for any purpose involving the making of a determination about the individual to whom they pertain; not merely that the agency does not engage in such uses.

"Disclosure of statistical records [to the individual] in most instances would not provide any benefit to anyone, for these records do not have a direct effect on any given individual; it would, however, interfere with a legitimate, Congressionally-sanctioned activity." (House Report 93-1416, p.19)

EXEMPTION FOR INVESTIGATORY MATERIAL COMPILED FOR DETERMINING SUITABILITY FOR FEDERAL EMPLOYMENT OR MILITARY SERVICE

> Subsection (k)(5) "Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;"

This provision permits an agency to exempt material from the individual access provision of the Act which would cause the identity of a confidential source to be revealed only if all of the following conditions are met:

- the material is maintained only for purposes of determining an individual's qualifications, eligibility or suitability for military service, employment in the civilian service or on a Federal contract, or access to classified material. By implication, employment would include appointments to Federal

advisory committees or to membership agencies, whether or not salaried;

- the material is considered relevant and necessary to making a judicious determination as to qualifications, eligibility or suitability and could only be obtained by providing assurance to the source that his or her identity would not be revealed to the subject of the record; e.g., for "critical sensitive positions;" and

- disclosure of the record with the identity of the source removed would likely reveal the identity of the source; e.g., the record contains information which could only have been furnished by one of several individuals known to the subject.

(Since information collected prior to the effective date of the Act may have been gathered under an implied promise of confidentiality, that pledge may be honored and those records exempted if the other criteria are met).

See subsection (k)(2), above, for a more extensive discussion of the circumstances under which records may be withheld to protect the identity of a confidential source.

This language was included to take into account the fact that the screening of personnel to assure that only those who are properly qualified and trustworthy are placed in governmental positions will, from time to time, require information to be collected under a pledge of confidentiality. Such pledges will be limited only to the most compelling circumstances; i.e.,

- without the information thus obtained, unqualified or otherwise unsuitable individuals might be selected; or

- the potential source would be unwilling to provide needed information without a guarantee that his or her identity will not be revealed to the subject; or

- to be of value in the personnel screening and often highly competitive assessments in which it will be used, the information must be of such a degree of frankness that it can only be obtained under an express promise that the identity of its source will not be revealed.

The Civil Service Commission and the Department of Defense (for military personnel) will issue regulations establishing procedures for determining when a pledge of confidentiality is to be made and otherwise to implement this subsection. These regulations and any implementing procedures will <u>not</u> provide that all information collected on individuals being considered for any particular category of positions will automatically be collected under a guarantee that

the identity of the source will not be revealed to the subject of the record.

This provision has been among the most misunderstood in the Act. It should be noted that it grants authority to exempt records only under very limited circumstances. "It will not be the customary thing to make these promises of confidentiality, so that most all of the information [in investigatory records] will be made available." (Congressional Record , November 20, 1974, p. 10887).

The term "Federal contracts" covers investigatory material on individuals being considered for employment on an existing Federal contract as well as investigatory material compiled to evaluate the capabilities of firms being considered in a competetive procurement.

EXEMPTION FOR TESTING OR EXAMINATION MATERIAL

> Subsection (k)(6) "Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process;"

This provision permits an agency to exempt testing or examination material used to assess the qualifications of an individual for appointment or promotion in the military or civilian service only if disclosure of the record to the individual would reveal information about the testing process which would potentially give an individual an unfair competitive advantage. For example, the Civil Service Commission and the military departments give written examinations which cannot be revised in their entirety each time they are offered. Access to the examination questions and answers could give an individual an unfair advantage. This language also covers certain of the materials used in rating individual qualifications. This subsection permits the agency to withhold a record only to the extent that its disclosure would reveal test questions or answers or testing procedures.

It was not the intent of this subsection to permit exemptions of information which are required to be made available to employees or members or are, in fact, made available to them as a matter of current practice. The presence of exemption (k) (7) is an indication of the intended narrow coverage of the exemptions set forth in (k) (6) and, similarly, the exemptions of (k) (7) and (k) (6) indicate the intended narrow coverage of the exemption set forth is subsection (k) (5).

EXEMPTION FOR MATERIAL USED TO EVALUATE POTENTIAL FOR PROMOTION IN THE ARMED SERVICES

> Subsection (k)(7) "Evaluation material used to determine potential for promotion in the armed services, but only to the

extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence."

The discussions of subsection (k)(2) and (5), above, should be reviewed in applying this provision. The same rationale regarding when and how the confidentiality of sources may be protected applies here.

The military departments will publish regulations specifying those categories of positions in the Armed Services for which pledges of confidentiality may be made when obtaining information on an individual's suitability for promotion. These categories will be narrowly drawn.

63-619 O - 76 - 71

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (l)

ARCHIVAL RECORDS

This subsection addresses the maintenance of those records which are transferred to the General Services Administration. It should be noted that there is a substantial difference between

- records which have been placed in records centers operated by the Administrator of General Services for "storage, processing and servicing" pursuant to Section 3103 of Title 44; and

- records which are accepted by the Administrator of General Services "for deposit in the National Archives of the United States [because they] have sufficient historical or other value to warrant their continued preservation by the United States Government" pursuant to Section 2103 of Title 44.

The former, those for which the General Services Administration is essentially a custodian, are addressed in subsection (l)(1). The latter, archival records which have been transferred to the Archives and are maintained by the Archivist, are addressed in subsections (l)(2) and (l)(3).

RECORDS STORED IN GSA RECORDS CENTERS

> Subsection (l)(1) "Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section."

Records which are sent to the General Services Administration for storage as a result of a determination by the agency head that to do so would "effect substantial economies or increase operating efficiency," (44 U.S.C 3103), are deemed to be part of the records of the agency which sent them and are subject to the Act to the same extent that they would be if maintained on the agency's premises.

This language, in effect, constitutes a clarification of the term "maintain" (subsection (a)(3)) with respect to records which have been physically transferred to GSA for storage. While records are stored in a records center, the agency which sent them to storage remains accountable for them and the General Services Administration

effectively functions as an agent of that agency and maintains them pursuant to rules established by that agency.

Records stored in records centers often constitute the inactive portion of systems of records, the remainder of which are kept on agency premises; e.g., agency payroll and personnel records. Whenever practicable, these inactive records should be treated as part of the total system of records and be subject to the same rules and procedures. In no case may they be subject to rules which are inconsistent with the Privacy Act.

To assure the orderly and effective operation of the records center and consistent with its authority to issue regulations governing Federal agency records management policies (under title 44 of the United States Code), the Privacy Act and these guidelines; the General Services Administration shall issue general guidelines to the agencies on preferred methods for handling systems of records stored in Federal records centers. In view of the intent underlying this provision, agencies may consider that the records stored in Federal records centers are transferred intra-agency and need not publish notice of "routine uses" to enable these transfers.

RECORDS ARCHIVED PRIOR TO SEPTEMBER 27, 1975

> Subsection (l)(2) "Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States Government as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register."

Records transferred to the Archives for "preservation" pursuant to 44 U.S.C. 2103, prior to September 27, 1975 are considered to be maintained by the Archives but are not subject to other provisions of the Act.

However, the National Archives is required to issue general notices describing its current holdings which cover, to the extent applicable, the elements specified in subsection (e)(4). These should include, as a minimum -

- the categories of individuals on whom records are maintained;
- the types of information in these records; and
- policies governing access and retrieval.

"It is intended that the notice provision not be applied separately and specifically to each of the many thousand of separate systems of

records transferred to the Archives prior to the effective date of this Act, but rather that a more general description be provided which pertains to meaningful groupings of record systems." (Congressional Record , December 18, 1974, p. H12245)

If, for any reason, a record currently in the Archives is disclosed to an agency for use by that agency in making a determination as to the rights, benefits, or entitlements of an individual, it becomes subject to the provisions of the Act to the same extent as any other record maintained by that agency.

RECORDS ARCHIVED ON OR AFTER SEPTEMBER 27, 1975

> Subsection (l)(3) "Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section."

Records transferred to the Archives pursuant to 44 U.S.C. 2103 (for "preservation") on or after September 27, 1975 are considered to be maintained by the Archives for purposes of the Act but are only subject to selected provisions of the Act."[They] are subject only to those provisions of this Act requiring annual public notice of the existence and character of the information systems maintained by the Archives, establishment of appropriate safeguards to insure the security and integrity of preserved personal information, and promulgation and implementation of rules to insure the effective enforcement of those safeguards." (Congressional Record , December 18, 1974, p. H12245).

The notice required for these records is on a system by system basis. "Since the records would already have been organized in conformity with the requirements of this section by the agency transferring them to the Archives, maintaining them in continued conformity with this law would not require any special effort." (House Report 93-1416, p. 20)

The exclusion of archival records from the provisions of the Act establishing the right to have access or to amend a record was also discussed in the House Report:

> "Records under the control of the Archives would not, however, be subject to the provisions of this law which permit changes in documents at the request of the individual named in them. A basic archival rule holds that archivists may not remove or amend

information in any records placed in their custody. The principle of maintaining the integrity of records is considered one of the most important rules of professional conduct. It is important because historians quite properly want to learn the true condition of past government records when doing research; they frequently find the fact that a record was inaccuarate is at least as important as the fact that a record was accurate.

"The Committee believes that this rule is eminently reasonable and should not be breached even in the case of individually identifiable records. Once those documents are given to the Archives, they are no longer used to make any determination about any individual, so amendment of them would not aid anyone. Furthermore, the Archives has no way of knowing the true state of contested information, since it does not administer the program for which the data was collected; it cannot make judgments as to whether records should be altered." (House Report 93-1416, p.21).

The Archivist is required to establish rules of conduct for GSA personnel to assure that records in the Archives are used only in a manner consistent with 44 U.S.C. 2103 and that Archives personnel are properly instructed in the rules governing access to and use of archival records.

However, when a record which has been deposited in the Archives is disclosed to an agency and becomes part of any agency's records which could be used in making a determination about an individual, that record would again be subject to the other applicable provisions of the Act.

Subsection (m)
GOVERNMENT CONTRACTORS

Subsection (m) "When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency."

The extent to which the provisions of the Act would apply to records other than those physically maintained by Federal agency personnel was one of the principal areas of difference between the Senate and House privacy bills (S. 3418 and H.R. 16373).

"The Senate bill would have extended its provisions outside the Federal government only to those contractors, grantees or participants in agreements with the Federal government, where the purpose of the contract, grant or agreement was to establish or alter an information system. It addressed a concern over the policy governing the sharing of Federal criminal history information with State and local government law enforcement agencies and for the amount of money which has been spent through the Law Enforcement Assistance Administration for the purchase of State and local government criminal information systems.

"The compromise amendment would now permit Federal law enforcement agencies to determine to what extent their information systems would be covered by the Act and to what extent they will extend that coverage to those with which they share that information or resources.

"At the same time it is recognized that many Federal agencies contract for the operation of systems of records on behalf of the agency in order to accomplish an agency function. It was provided therefore that such contracts if agreed to on or after the effective date of this legislation shall provide that those contractors and any employees of those contractors shall be considered to be employees of an agency and subject to the provisions of the legislation." (Congressional Record , Dec. 17, 1974, p. S21818)

It was also agreed that the Privacy Protection Study Commission should be directed to study the applicability of the provisions of the Privacy Act to the private sector and make recommendations to the Congress and the President (See Subsection 5(b) of the Act).

The effect of this provision is to clarify, further, the definition of the term "maintain" as it establishes agency accountability for systems of records. (See subsection (a)(3)). It provides that systems operated under a contract which are designed to accomplish an agency function are, in effect, deemed to be maintained by the agency. It was not intended to cover private sector record keeping systems but to cover de facto as well as de jure Federal agency systems.

"Contract" covers any contract, written or oral, subject to the Federal Procurement Regulations (FPR's) or Armed Services Procurement Regulations (ASPR's), but only those which provide "... for the operation by or on behalf of the agency of a system of records to accomplish an agency function ..." are subject to the requirements of the subsection. While the contract need not have as its sole purpose the operation of such a system, the contract would normally provide that the contractor operate such a system formally as a specific requirement of the contract. There may be some other instances when this provision will be applicable even though the contract does not expressly provide for the operation of a system; e.g., where the contract can be performed only by the operation of a system. The requirement that the contract provide for the operation of a system was intended to ease administration of this provision and to avoid covering a contractor's system used as a result of his management discretion. For example, it was not intended that the system of personnel records maintained by large defense contractors be subject to the provisions of the Act.

Not only must the terms of the contract provide for the operation (as opposed to design) of such a system, but the operation of the system must be to accomplish an agency function. This was intended to limit the scope of the coverage to those systems actually taking the place of a Federal system which, but for the contract, would have been performed by an agency and covered by the Privacy Act. Information pertaining to individuals may be maintained by an agency (according to subsection (e)(1)) only if such information is relevant and necessary to a purpose of the agency required to be accomplished by statute or Executive order of the President. Although the statute or Executive order need not specifically require the creation of a system of records from this information, the operation of a system of records required by contract must have a direct nexus to the accomplishment of a statutory or Presidentially directed goal.

If the contract provides for the operation of a system of records to accomplish an agency function, then "... the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system."

The clause "...consistent with its authority ..." makes it clear that the subsection does not give an agency any new authority additional to what it otherwise uses. The subsection clearly imposes new responsibilities upon an agency but does not confer any new authority to implement it. Although the method by which agencies cause the requirements of the section to be applied to systems is not set forth, the manner of doing so must be consistent with the agency's existing authority. The method of causing was envisioned to be a clause in the contract, but as with the "Buy America" provision in Government contracts, the breach of the clause was not necessarily intended to

result in a termination of the contract. In addition, several of the requirements of the Privacy Act are simply not applicable to systems maintained by contractors, and this clause was a method of indicating that an agency was not required to impose those new standards. Agencies were given some discretion in determining the method or methods by which they would cause the otherwise applicable requirements to be applied to a system maintained under contract. This subsection does not merely require that an agency include provisions consistent with the Privacy Act in its contracts. It requires, in addition, that the agency cause the requirements of the Act to be applied, limited only by its authority to do so. Because of this agency accountability--which underlies many of the provisions of the Privacy Act--there should be an incentive for an agency to cause its contractors who are subject to this subsection to apply the requirements of the section in a manner which is enforceable. Otherwise, the agencies may end up performing those functions in order to satisfy the activity of the "cause" requirement.

The decision as to whether to contract for the operation of the system or to perform the operation "in-house" was not intended to be altered by this subsection. Furthermore, this subsection was not intended to significantly alter GSA and OMB authority under the Brooks Act (P.L. 89-306) or Executive Order No. 11717 dated May 9, 1973, concerning the method of ADP procurement. The principles concerning reliance upon the private sector in OMB Circular No. A-76, and related provisions were also not intended to be changed.

The provisions would apply to all systems of records where, for example-

- the determinations on benefits are made by Federal agencies;
- the records are maintained for administrative functions of the Federal agency such as personnel, payroll, etc; or
- health records being maintained by an outside contractor engaged to provide health services to agency personnel.

The provisions would not apply to systems of records where:

- records are maintained by the contractor on individuals whom the contractor employs in the process of providing goods and services to Federal government.

- an agency contracts with a state or private educational organization to provide training and the records generated on contract students pursuant to their attendance (admission forms, grade reports) are similar to those maintained on other students and are comingled with their records on other students.

When a system of records is to be operated by a contractor on behalf of an agency for an agency function, the contractual instrument must specify, to the extent consistent with the agency's authority to require it, that those records be maintained in accordance with the Act. Agencies will modify their procurement procedures and practices to ensure that all contracts are reviewed before award to determine whether a system of records within the scope of the Act is being contracted for and, if so, to include appropriate language regarding the maintenance of any such systems.

For systems operated under contracts awarded on or after September 27, 1975, contractor employees may be subject to the criminal penalties of subsections (i) (1) and (2) (for disclosing records the disclosure of which is prohibited by the Act or for failure to publish a public notice). Although the language is not clear on this point, it is arguable that such criminal liability only exists to the extent that the contractual instrument has stipulated that the provisions of the Act are to be applied to the contractually maintained system. However, an agency which fails, within the limits of its authority, to require that systems operated on its behalf under contracts, may be civilly liable to individuals injured as a consequence of any subsequent failure to maintain records in conformance with the Act. The reference to contractors as employees is intended only for purposes of the requirements of the Act and not to suggest that, by virtue of this language, they are employees for any other purposes.

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (n)

MAILING LISTS

Section (n) "An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public."

The language in this section is susceptible of various interpretations and must be read in the context of relevant legislative history. It is clear, however, that this provision seeks to reach the sale or rental of lists of names and addresses for commercial or other solicitation purposes not related to the purposes for which the information was collected.

"Language included in the legislation would prohibit the sale or rental of mailing lists, names and addresses, by Federal agencies maintaining them. The philosophy behind this amendment is that the Federal Government is not in the mailing list business, and it should not be Federal policy to make a profit from the routine business of government, particularly when the release of such lists has been authorized under the Freedom of Information Act. In other words, such lists can not be withheld by an agency, unless it determines that the release would constitute a clearly unwarranted invasion of privacy under section 552 (b)(6) of title 5, United State Code.

"Thus, the language of the bill before us does not ban the release of such lists where either sale or rental is not involved." (Congressional Record , December 18, 1974 p. H 12246)

? While the reference to the FOIA speaks only of "a clearly unwarranted invasion of personal privacy" (see 5 U.S.C. 552 (b)(6)) agencies may presumably withhold lists of names and addresses from the public under any of the exemptions to the FOIA (5 U.S.C. 552 (b)) when they deem it appropriate to do so.

It is apparent that what is prohibited is "sale or rental" of such lists and the langage may be read to prohibit "the sale or rental of lists of names and addresses by Federal agencies unless the sale or rental is specifically authorized by law . [emphasis added]." (Senate Report 93-1183, p. 31)

The Senate report, when read in combination with the House floor discussion cited above, suggests that agencies may not sell or rent mailing lists for commercial or solicitation purposes unless they are authorized specifically by law to sell or rent such lists. It is equally apparent that this language in no way creates an authority to withhold any records otherwise required to be disclosed under the Freedom of Information Act (5. U.S.C 552). It is problematic whether

the language "may not be sold or rented" precludes the charging of fees authorized under the Freedom of Information Act. It would seem reasonable to conclude that fees permitted to be charged for materials required to be disclosed under the Freedom of Information Act are not precluded and that lists, such as agency telephone directories, which are currently sold to the public by the Superintendent of Documents can continue to be sold.

Finally, this provision appears not to have been intended to reach the disclosure of names and addresses to agencies or other organizations other than for commercial or solicitation purposes. Other disclosure (e.g., the disclosures of names and addresses for a statistical study or to issue checks) would be subject to the requirements of section (b).

PRIVACY ACT GUIDELINES - July 1, 1975

Section (o)
REPORT ON NEW SYSTEMS

Section (o) "Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers."

This subsection is intended to assure that proposals to establish or modify systems of records are made known in advance so that

- there is a basis for monitoring the development or expansion of agency record-keeping activity,

- the Commission established by section 5 can review trends in the use of personal information and the application of technology.

This provision resulted from the discussions surrounding the need for an independent agency to regulate and oversee the implementation of the Act:

"The compromise amendment still would require that agencies provide adequate advance notice to the Congress and to the Office of Management and Budget of any proposal to establish or alter a system of records in order to permit an evaluation of the privacy impact of that proposal. In addition to the privacy impact, consideration should be given to the effect the proposal may have on our Federal system and on the separation of powers between the three branches of government. These concerns are expressed in connection with recent proposals by the General Services Administration and Department of Agriculture to establish a giant data facility for the storing and sharing of information between those and perhaps other departments. The language in the Senate report reflects the concern attached to the inclusion of this language in S.3418." (Senate Report 93-1183, page 64-66).

"The acceptance of the compromise amendment does not question the motivation or need for improving the Federal government's data gathering and handling capabilities. It does express a concern, however, that the office charged with central management and oversight of Federal activities and the Congress have an opportunity to examine the impact of new or altered data systems on our citizens, the provisions for confidentiality and security in those systems and the extent to which the creation of the system will alter or change interagency or intergovernmental relationships related to information programs." (Congressional Record , December 17, 1974, p. S 21818)

A report is required to be submitted for each proposed new system of records and for changes to existing systems. The criteria for determining what constitutes a change in an existing system requiring the preparation of a report under this subsection are substantially the same as those discussed under subsection (e)(4), the public notice; namely any change which:

- increases the number or types of individuals on whom records are maintained;
- expands the type or amount of information maintained;
- increases the number or categories of agencies or other persons who may have access to those records;
- alters the manner in which the records are organized so as to change the nature or scope of those records; e.g., the combining of two or more existing systems;
- modifies the way in which the system operates or its location(s) in such a manner as to alter the process by which individuals can exercise their rights under the Act; e.g., to seek access or request amendment of a record; or
- changes the equipment configuration on which the system is operated so as to create the potential for greater access; e.g., adding a telecommunications capability.

The reports required under this section are to be submitted to the Congress, to the Director of the Office of Management and Budget (Attn: Information Systems Division) and to the Privacy Protection Study Commission.

The Office of Management and Budget will issue, under separate cover, more detailed guidance on the format, timing, and content of the reports.

PRIVACY ACT GUIDELINES - July 1, 1975

Subsection (p)

ANNUAL REPORT

Subsection (p) "The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section."

This subsection provides that the President submit to the Congress a list of systems exempted from the Act under the terms of section (j) or (k). "Also to be included in the annual report would be the reasons for such exemptions and other information indicating efforts to comply with the law. It is hoped that all such information would be made public. If, however, the nature of any such exemption requires a security classification marking, it should be placed in a separate part of the report so as not to affect the remainder of the annual report." (House Report 93-1416, p. 21).

Agencies will be required to prepare reports to the Office of Management and Budget (Attn: Information Systems Division) by April 30 of each year (beginning April 30, 1976) covering their activities under the Act during the preceding calendar year. The Office of Management and Budget will analyze data contained in the agency reports and prepare the required Presidential report to the Congress. The information required in the individual agency reports will include not only the minimum information required for inclusion in the report to Congress but also such information as is needed to evaluate the overall effectiveness of the Privacy Act implementation, identify areas in which implementing policies or procedures should be changed, and assess the impact of Federal data management activities.

Agency reports shall include but not be limited to the following:

- Summary - A brief management summary of the status of actions taken to comply with the Act, the results of these efforts, any problems encountered and recommendations for any changes in legislation, policies or procedures.

- Accomplishments - A summary of major accomplishments; i.e., improvements in agency information practices and safeguards.

- Plans - A summary of major plans for activities in the upcoming year, e.g., area of emphasis, additional securing of facilities planned.

- Exemptions - A list of systems which are exempted during the year from any of the operative provisions of this law permitted under the terms of subsections (j) and (k), whether or not the exemption was obtained during the year, the number of records in each system exempted from each specific provision and reasons for invoking the exemption.

- Number of systems - A brief summary of changes to the total inventory of personal data systems subject to the provisions of the Act including reasons for major changes; e.g. the extent to which review of the relevance of and necessity for records has resulted in elimination of all or portions of systems of records or any reduction in the number of individuals on whom records are maintained. Agencies will also be requested to provide OMB with a detailed listing of all their systems of records, the number of records in each and certain other data to facilitate oversight of the implementation of the Act. (Detailed reporting procedures will be issued under separate cover.)

- Operational Experiences - A general description of operational experiences including estimates of the number of individuals (in relation to the total number of records in the system) requesting information on the existence of records pertaining to them, refusing to provide information, requesting access to their records, appealing initial refusals to amend records, and seeking redress through the courts.

More extensive data will be requested on those cases where the agency was unable to comply with the requirements of the Act or these guidelines; e.g., access was not granted or a request to amend could not be acknowledged within prescribed time limits.

More detailed instructions on the format, content and timing of these reports will be issued by OMB.

PRIVACY ACT GUIDELINES - July 1, 1975

Section (q)

EFFECT OF OTHER LAWS

Subsection (q) "No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section."

This provision makes it explicit that an individual may not be denied access to a record pertaining to him under subsection (d)(1), access to records, because that record is permitted to be withheld from members of the public under the Freedom of Information Act. The only grounds for denying an individual access to a record pertaining to him are the exemptions stated in this Act, subsections (j) and (k), and subsection (l) archival records. In addition consideration may have to be given to other statutory provisions which may govern specific agency records.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

GOVERNMENT SPECIFICATIONS COMM.
RECEIVED
OCT 14 1975
WASHINGTON, D. C. 20510

September 30, 1975

CIRCULAR NO. A-108
Transmittal Memorandum No. 1

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Responsibilities for the maintenance of records about individuals by Federal agencies

1. Purpose. This supplement to OMB Circular A-108 dated July 1, 1975 provides guidance to Federal agencies regarding the preparation and submission of reports of their intention to establish or alter systems of personal records as required by the Privacy Act of 1974 (P.L. 93-579, 5 U.S.C. 552a(o)). These procedures supersede preliminary guidance on preparing the Report on New Systems contained in the OMB Privacy Act Guidelines dated July 1, 1975 (Federal Register, July 9, 1975, p. 28977).

2. Reporting requirements.

a. A Report on New Systems must be submitted when:

(1) A new system of personal records subject to the Privacy Act is proposed. A new system of records subject to the new system reporting requirement is one for which no public notice consistent with the provisions of subsection (e)(4) is currently published in the Federal Register.

If a public notice for any specific system of records is withdrawn, suspended, cancelled, or terminated and subsequently reinstated, the subject system of records shall be considered a new system and subject to the new system reporting requirement at such time that it is reinstated.

(2) A change to a system of personal records subject to the Privacy Act is proposed. A new system report is required for any change to an existing system which meets any of the following criteria.

63-619 O - 76 - 72

(a) Increase or change the number or types of individuals on whom records are maintained. Changes involving the number (rather than the types) of individuals about whom records are kept need only be reported when that change significantly alters the character and purpose of the system of records, e.g., normal increases in historical files or other increases in the number of records in a file which can be attributed to normal growth patterns need not be reported. A change resulting from a change in the scope of the population covered; e.g., a system which only covered a portion of the work force is expanded to cover all, is required to be reported.

(b) Expand the type or categories of information maintained. For example, if an employee payroll file is expanded to include data on education and training, this would be considered an expansion of the "type or categories of information" maintained, and would have to be reported.

(c) Alter the manner in which the records are organized or the manner in which the records are indexed or retrieved so as to change the nature or scope of those records. For example, the combining of two or more existing systems or splitting an existing system into two or more different systems such as might occur in a centralization or decentralization of organizational responsibilities would require a report.

(d) Alter the purposes for which the information is used. For example, a proposal that files currently used as historical military service records are to be used for making determinations on eligibility for disability benefits would require a report. A proposal to establish or change the "routine uses" of the system will not require the submission of a Report on New System if such use is compatible with the purposes for which the system is maintained; i.e., does not, in effect, create a new purpose. Any new or changed "routine use" would, however, be subject to the requirements to give 30 days prior notice of such change in the Federal Register (5 U.S.C. 552a(e)(11)).

(e) Change the equipment configuration (i.e., hardware and/or software) on which the system is operated so as to create the potential for either greater or easier access. For example, the addition of a telecommunications

capability which could increase the risk of unauthorized access would require a report.

b. Content of the Report. The agency report on proposed new systems, or proposal to modify existing systems shall consist of a brief narrative description, supporting documentation and an update of the inventory of Federal personal data systems as outlined below:

(1) Narrative Statement - A brief statement, normally not to exceed four pages in length, which:

-- describes the purposes of the system of records.

-- identifies the authority under which the system of records is to be maintained.

-- provides the agency's evaluation of "the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals and its effect on the preservation of the constitutional principle of federalism and separation of power," and

-- provides a brief description of steps taken by the agency to minimize the risk of unauthorized access to the system of records including a discussion of higher or lower risk alternatives which were considered for meeting the requirements of the system. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be available on request.

The narrative statement should make reference, as appropriate, to information in the supporting documentation rather than restate such information.

Where changes to computer installations, communications networks, or any other general changes in information collection, handling, storage or dissemination are made which affect multiple systems of records; a single consolidated new system report may be submitted. In such cases, the narrative statement should address the overall privacy implications of the proposed change, identify all systems of records affected by the change and briefly describe any unique impacts on any specific system of

records. Supporting documentation, as defined in the subsequent paragraphs, shall be provided for each system of records.

(2) Supporting Documentation - The following shall be appended to all new system reports:

(a) An advance copy of the new or revised system notice (consistent with the provisions of 5 U.S.C. 552a(e)(4)) which the agency proposes to publish for the new or altered system(s). For proposed alterations of existing systems the documentation should be provided in the same form as the agency proposes to publish the public notice of such changes. If the agency proposes to publish changes in the form of a revision to the public notice, a copy of the proposed notices of revision should be provided. If the agency plans to supersede the entire existing notice, changes from the currently published notice shall be highlighted by underlining all new or revised portions.

(b) An advance copy of any new rules or changes to published rules (consistent with the provisions of 5 U.S.C. 552a(e)(11) and (f)) which the agency proposes to issue for the new or altered system. If no change to existing rules are required for the proposed new or altered system, the report shall so state. Proposed changes to existing rules shall be provided in a manner similar to that described for the system notices.

(c) An advance copy of any proposed rules setting forth the reasons why the system is to be exempted from any specific provision, (consistent with the provisions of 5 U.S.C. 552a(j) or (k)) if the agency head plans to invoke any exemptions for the new or altered systems.

(3) Update of Federal Inventory of Personal Data Systems - OMB in cooperation with the National Archives and Records Service is developing a perpetual inventory of all systems of records subject to the Act. The detailed plans for this inventory are still being developed. It is anticipated, however, that agencies will be requested to provide a simple report to facilitate maintenance of the Federal inventory. This portion of the report on new systems is not in effect until such time as further instructions are issued.

c. Report Format.

(1) Narrative Statement. No standard format has been established for the narrative statement. Agencies should present the information requested in the most concise fashion possible.

(2) Supporting Documentation. The format of the documentation shall, where applicable, be consistent with the publication requirements established by the Office of the Federal Register of the General Services Administration.

(3) Update of Federal Inventory of Personal Data Systems. Format being developed.

d. Distribution of Report. Two copies of each new systems report shall be submitted to each of the following:

(1) Speaker of the House.

(2) President of the Senate.

(3) The Privacy Protection Study Commission during the period of its existence as set forth in Section 5(g) of the Privacy Act.

(4) Office of Management and Budget.

e. Timing. A report on a proposed new or altered system of records shall be submitted no later than the following dates, whichever is earlier:

(1) Sixty (60) days before any issuance of data collection forms and/or instructions; or

(2) Sixty (60) days before any public issuance of a Request for Proposal or an Invitation to Bid for computer and/or communications systems or services intended to support the system of records.

3. Effective Date. The provisions of this Transmittal Memorandum are effective upon issuance.

4. Inquiries. Inquiries concerning this Transmittal Memorandum may be addressed to the Information Systems Division, Office of Management and Budget, Room 9002, NEOB, Washington, D.C. 20503, telephone 202 395-4814.

JAMES T. LYNN
DIRECTOR

(No. A-108)

OFFICE OF MANAGEMENT AND BUDGET

Implementation of the Privacy Act of 1974

SUPPLEMENTARY GUIDANCE

NOVEMBER 21, 1975.

This material is provided to address comments and questions of general interest raised since the release of the Office of Management and Budget's guidelines for implementing section 3 of the Privacy Act of 1974. (FEDERAL REGISTER, Volume 40, Number 132, dated July 9, 1975, pp. 28949–28978.)

Additional supplements will be issued as necessary.

JAMES T. LYNN, *Director.*

1. *Definition of System of Records* (5 U.S.C. 552a(a)(5)). On page 28952, third column, after line 27, add:

"Following are several examples of the use of the term 'system of records';

"Telephone directories. Agency telephone directories are typically derived from files (e.g., locator cards) which are, themselves, systems of records. For example, agency personnel records may be used to produce a telephone directory which is distributed to personnel of the agency and may be made available to the public pursuant to 5 U.S.C. 552a(b) (1) and (2), (intra-agency and public disclosure, respectively). In this case the directory could be a disclosure from the system of records and, thus, would not be a separate system. On the other hand, a separate directory system would be a system of records if it contains personal information. A telephone directory, in this context, is a list of names, titles, addresses, telephone numbers, and organizational designations. An agency should not utilize this distinction to avoid the requirements of the Act including the requirement to report the existence of systems of records which it maintains.

"Mailing lists. Whether or not a mailing list is a system of records depends on whether the agency keeps the list as a separate system. Mailing lists derived from records compiled for other purposes (e.g., licensing) could be considered disclosures from that system and would no be systems of records. If the system from which the list is produced is a system of records, the decision on the disclosability of the list would have to be made in terms of subsection (b) (conditions of disclosure) and subsection (n) (the sale or rental of mailing lists). A mailing list may, in some instances, be a stand-alone system (i.e., subscription lists) and could be a system of records subject to the Act if the list is maintained separately by the agency, it consists of records (i.e., contains personal information), and information is retrieved by reference to name or some other identifying particular.

"Libraries. Standard bibliographic materials maintained in agency libraries such as library indexes, Who's Who volumes and similar materials are not considered to be systems of records. This is *not* to suggest that all published materiasl is, by virtue of that fact, not subject to the Act. Collections of newspaper clippings or other published matter about an individual maintained other than in a conventional reference library would normally be a system of records."

2. *Routine Uses—Intra-agency disclosures* (5 U.S.C. 552a(a)(7))

On page 28953, first column, after line 17, add:

"Intra-agency transfer need not be considered routine uses. Earlier versions of House privacy bills, from which the routine use concept derives, permitted agencies to disclose records within the agency to personnel who had a need for such access in the course of their official duties thus permitting intra-agency disclosure without the consent of the individual. The concept of routine was developed to permit other than intra-agency disclosures after it became apparent that a substantial unnecessary workload would result from having to seek the consent of the subject of a record each time a transfer was made for a purpose '. . . compatible with the purpose for which [the record] was collected' (5 U.S.C. 552a(a)(7)). To deter promiscuous use of this concept, a futher provision was added requiring that routine uses be subject to public notice. (5 U.S.C. 522a(e)(11).) It is our view that the concept of routine use was devised to cover disclosures other than those to officers or employees who have a need to for the record in the performance of their official duties within the agency.

"It is not necessary, therefore, to include intra-agency transfers in the portion of the system notice covering routines uses (5 U.S.C. 522a(e)(4)(D)) but agencies may, at their option, elect to do so. The portion of the system notice covering storage, retrievability, access controls, rentention and disposal (5 U.S.C. 522a(e)(4)(E)) should describe the categories of agency officials who have access to the system."

3. *Consent for access in response to congressional inquiries* (5 U.S.C. 522a(b)(9))

On page 28955, third column, after line 18, add:

To assure that implementation of the Act does not have the unintended effect of denying individuals the benefit of congressional assistance which they request, it is recommended that each agency establish the following as a routine use for all of its systems, consistent with subsections (a)(7) and (e)(11) of the Act:

Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

The operation of this routine use will obviate the need for the written consent of the individual in every case where an individual requests assistance of the Member which would entail a disclosure of information pertaining to the individual.

In those cases where the congressional inquiry indicates that the request is being made on behalf of a person other than the individual whose record is to be disclosed, the agency should advise the congressional office that the written consent of the subject of the record is required. The agency should not contact the subject unless the congressional office reqeusts it to do so.

In addition to the routine use, agencies can, of course, respond to many congressional requests for assistance on behalf of individuals without disclosing personal information which would fall within the Privacy Act, e.g., a congressional inquiry concerning a missing Social Security check can be answered by the agency by stating the reason for the delay.

Personal information can be disclosed in response to a congressional inquiry without written consent or operation of a routine use—

If the information would be required to be disclosed under the Freedom of Information Act (Subsection (b)(2));

If the Member requests that the response go directly to the individual to whom the record pertains;

In "compelling circumstances affecting the health or safety of an individual * * *" (Subsection (b)(8)); or

To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof * * *" (Subsection (b)(9)).

The routine use recommended above and disclosures thereunder are, of course, subject to the 30 day prior notice requirement of the Act (Subsection (e)(11)). In the interim, however, it should be possible to respond to most inquiries by using the provisions cited in the previous paragraph. Furthermore, when the congressional inquiry indicates that the request is being made on the basis of a written request from the individual to whom the record pertains, consent can be inferred even if the constituent letter is not provided to the agency.

"This standard for implied consent does not apply to other than congressional inquiries."

4. *Describing the purpose in the accounting of disclosures* (Subsection (c)(1))

On page 28956, first column, after line 42, add:

"Agencies which submit inquiries to other agencies in connection with law enforcement or pre-employment investigations (e.g., record checks) are reminded to include the purpose in their record check in order to preclude having record checks returned to them to ascertain the purpose of the check. It is noted that this is necessary whether the inquiry is made pursuant to the subsection (b)(3) or (b)(7) ('routine use' or law enforcement disclosures). At a minimum, the inquiring agency must describe the purpose as either a background or law enforcement check."

5. *Agency procedures for review of appeals of denials of requests to amend a record* (Subsection (d)(3))

On page 28959, second column, after line 39, add:

"This does *not* mean that the officer on appeal must be a justice or judge.

Rather, the reviewing official designated by the agency head my be a justice or judge (unlikely in this case) or any other agency official who meets the criteria in 5 U.S.C. 2104a (1), (2), and (3)."

6. *Correcting records released to an individual* (Subsection (e)(6))

On page 28965, second solumn, after line 6, add:

"While this language requires that agencies make reasonable efforts to assure the accuracy of a record before it is disclosed, when an individual requests access to his or her record, pursuant to subsection (d)(1), above, the record must be disclosed without change or deletion except as permitted by subsections (j) and (k), exemptions. To avoid requiring individuals to file unnecessary requests for amendment, however, the agency should review the record and annotate any material discolsed to indicate that which it intends to amend or delete."

7. *Rights of parents and legal guardians* (Subsection (h))

On page 28970, second column, after line 59, add:

"This is not intended to suggest that minors are precluded from exercising rights on their own behalf. Except as otherwise provided in the Act (e.g., general or specific exemptions) a minor does have the right to access a record pertaining to him or herself. There is no abosolute right of a parent to have access to a record about a child absent a court order or consent."

8. *Relationships to the Freedom of Information Act* (Subsection (q))

On page 28978, third column, after the last line, add:

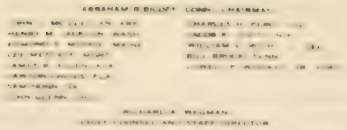
"In some instances under the Privacy Act an agency may (1) exempt a system of records (or a portion thereof) from access by individuals in accordance with the general or specific exemptions (subsection (j) or (k)); or (2) deny a request for access to records compiled in reasonable anticipation of a civil action or proceeding or archival records (subsection (d) (5) or (1)). In a few instances the exemption from disclosure under the Privacy Act may be interpreted to be broader than the Freedom of Information Act (5 U.S.C. 552). In such instances the Privacy Act should not be used to deny access to information about an individual which would otherwise have been *required* to be disclosed to that individual under the Freedom of Information Act.

"Whether a request by an individual for access to his or her record is to be processed under Privacy Act or Freedom of Information Act procedures involves several considerations. For example, while agencies have been encouraged to reply to requests for access under the Privacy Act within ten days wherever practicable, consistent with the Freedom of Information Act (FOIA), the Privacy Act does not establish time limits for responding to requests for access. (See discussion of subsection (d)(1).) The Privacy Act also does not require an administrative appeal on denial of access comparable to that under FOIA although agencies are encouraged to permit individuals to request an administrative review of initial denials of access to avoid, where possible, the need for unnecessary judicial action. It can also be argued that requests filed under the Privacy Act can be expected to be specific as to the system of records to which access is sought whereas agencies are required to respond to an FOIA request only if it 'reasonably describes' the records sought. Further, the Freedom of Information Act permits charging of fees for search as well as the making of copies while the Privacy Act permits charging only for the direct cost of making a copy upon request.

"It is our view that agencies should treat requests by individuals for information pertaining to themselves which specify either the FOIA or the Privacy Act (but not both) under the procedures established pursuant to the Act specified in the request. When the request specifies, and may be processed under, both the FOIA and the Privacy Act, or specifies neither Act, Privacy Act procedures should be employed. The individual should be advised, however, that the agency has elected to use Privacy Act procedures, of the existence and the general effect of the Freedom of Information Act, and of the differences, if any, between the agency's procedures under the two Act) (e.g., fees, time limits, access and appeals).

"The net effect of this approach should be to assure the individuals do not, as a consequence of the Privacy Act, have less access to information pertaining to themselves than they had prior to its enactment."

[FR Doc. 75-32297 Filed 12-3-75; 8:45 am]



United States Senate

COMMITTEE ON
GOVERNMENT OPERATIONS
WASHINGTON, D.C. 20510

October 6, 1975

Dear Colleague:

The Privacy Act of 1974 (Public Law 93-579) went into effect on September 27, 1975. This law significantly guards the right of privacy of all Americans and protects the millions of people who are the subject of government files from unwarranted disclosure.

Immediate concern has been expressed by many of our colleagues regarding the effect of the Privacy Act on the smooth processing of constituent case work by Members of Congress. The Office of Management and Budget, which is authorized to develop guidelines for implementation of the Act, had previously advised agencies on the relationship of the Act to Congressional inquiries on behalf of constituents. There has been confusion as to the appropriate method for handling Congressional case work under the Act.

Meetings were held during the past week with representatives of the Office of Management and Budget, the Department of Health, Education and Welfare, the Department of Defense and the Veterans Administration regarding their procedures for dealing with case work problems. A memorandum for heads of Executive Departments and Agencies reflecting an understanding which was reached at those meetings was issued today by OMB Director James Lynn stating the interim procedures that should be used in implementing the Act until more permanent procedures can be developed. This memorandum supercedes the September 26 memorandum from OMB on this subject.

The enclosed October 3 memorandum provides that in most cases during this interim, agencies may give certain categories of information to Congressional case workers because that information is not protected by the Act. For example, this might include the reason for the delay of a social security check and assurance it will be acted upon or given attention. Of the 2000 current cases being handled by the Army, DoD estimates only 50 would involve information protected by the Act.

In other instances, information may be provided as a result of an exception from individual consent already set forth in the Act, either because of compelling circumstances affecting the health or safety of an individual or because the information would be required to be disclosed under the Freedom of Information Act. All three agencies have agreed to provide each Congressional office with categories of information which they can give out without written request.

When an oral Congressional inquiry indicates that a request is being made on the basis of a written letter from the individual to whom the record pertains, consent should be inferred even if the constituent letter is not provided to the agency. In the case of an oral request to the Congressional office, the agency will proceed to process work on the problem and ask that the Congressional office obtain consent from the constituent or the agency should offer to transmit the information directly to the constituent with a letter indicating that it is being sent at the request of the Member of Congress.

We are hopeful that this procedure will substantially reduce any delay in the handling of case work for your constituents and that we can successfully begin to implement the Privacy Act.

Sincerely,

Jack Brooks

Abraham A. Ribicoff

Bella S. Abzug

Edmund S. Muskie

Charles H. Percy

NINETY-FOURTH CONGRESS
Congress of the United States
House of Representatives
GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS
SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS
RAYBURN HOUSE OFFICE BUILDING, ROOM B-349-B-C
WASHINGTON, D.C. 20515

Mr. Speaker:

When the Privacy Act of 1974 went into effect on Sept. 27, 1975, the capability of Members of Congress to perform services for their constituents was brought to a near halt. It is my view that some agencies deliberately interpreted the law to exclude access by Members to information on individuals.

Congress, its committees and subcommittees, the act says, have access to personally identifiable information if that information falls within the jurisdiction of the body. Members of Congress acting individually received no right under the act to see personal information from an individual's record. Executive branch interpretation prevented congressional offices from representing the very constituents we are elected to serve by stopping our access to agency records without specific written authorization from the subject of the records.

The act does provide that agencies can release information to persons other than the subject of the record if such release is routinely made and the decision to routinely release such information is published in the Federal Register. On Oct. 3, 1975, James Lynn, Director of OMB, issued the following guideline for agency consideration:

> Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of the individual.

Under this guideline, congressional offices need not write agencies for information nor show the agencies proof that a request has been received by that office. At the same time, the federal agencies are able to respond immediately to the congressional inquiries without obtaining the individual's consent and without the need to respond to the congressional office in writing. In substance, the OMB guideline, if observed by federal agencies simply allows congressmen to continue helping constituents as we had done before Sept. 27, 1975.

Unfortunately, troubles developed in the implementation of this OMB guideline, either because employees of executive branch agencies had not gotten the word that such release should be made, or because agencies refused to comply with the OMB guideline.

As chairwoman of the Subcommittee on Government Information and Individual Rights, I wrote to each federal agency at the end of 1975 urging compliance with the OMB guideline. If an agency felt it was impossible to be in conformity with the OMB guideline, I asked for an explanation as to why not.

A sample copy of the letter is appended.

I have received responses from 49 federal agencies out of a total 150 letters sent. Notably, the only Cabinet level department that failed to respond to my query is the Department of State. Others outstanding for their lack of response are the CIA, the SEC and the numerous boards, committees and commissions.

Of the agencies that responded to my inquiry, the Selective Service Administration is the only agency that has refused outright to comply with the guideline, based on its need to keep recruiting information in strictest confidence. The agency did state its desire to be responsive to all written congressional inquiries.

Four agencies hedged by saying they are studying the guideline, or that they won't refuse to deal with congressional inquiries. These were the Federal Power Commission, the Civil Rights Commission, the Federal Home Loan Board and the Federal Maritime Commission.

The chairman of this last body has "directed the Commission staff to draft an appropriate "routine use" provision to permit disclosures from the records of their constituents in response to a written request from members of Congress made on behalf of such constituents."

Four agencies had similar provisions in their guidelines already. For instance, the Commodity Futures Trading Commission makes information "available to any Member of Congress who is acting in his capacity as a Member of Congress."

The Community Services Administration discloses information routinely "to a member of Congress seeking information concerning the individual, but only when the individual is a constituent of the member and had requested assistance from the member with respect to the subject matter of the record."

The National Science Foundation and the Occupational Safety and Health Review Commission also make information routinely available to Members of Congress.

Five agencies said the guideline is not necessary or applicable to their operation. The Appalacian Regional Commission "does not make grants or provide other funds to individuals, therefore, we feel the regulations to which you refer do not apply to this agency."

The Federal Mediation and Conciliation Service has concluded that the agency can respond fully to "infrequent Congressional inquiries in these other areas within the rationale of the OMB recommendations without amending our existing regulation." The service will ask for a copy of the constituent's letter asking for aid or for assurance that the request from the constituent was in writing, presumably, all contained in a written inquiry from the congressional office. This is a particularly innovative evasion of the question and completely unresponsive to the OMB guideline, not even showing a need for written congressional inquiries.

The Indian Claims Commission simply stated that the only records it maintains pertaining to individuals are commission employee personnel records. No discussion was made of intention to comply with the OMB guidance.

Although the Smithsonian Institute has not seen fit to publish any Privacy Act guidelines in the Federal Register to date, I have been assured the OMB guideline has been circulated to several persons in the institute so no problems should arise regarding constituent casework.

The National Mediation Board states that its policy since the establishment of the board is to respond fully to all congressional inquiries and it will continue to, so no specific regulation is needed.

All other responding agencies are in some stage of implementing the guideline. Fourteen of these are in the process of adopting the guideline as an agency regulation and 17 have already done so. This includes HEW and its component, the Social Security Administration, the entire Department of Defense, the Veterans Administration and the General Services Administration which controls the Military Personnel Records facility and the National Personnel Records Center, both in St. Louis. NASA has agreed to implement the OMB guidance with the condition that the congressional inquiry be made in writing. No mention was made by NASA that the constituent inquiry should be in writing also.

I am in hopes that those agencies delinquent in responding to my inquiry will realize the importance of establishing a uniform policy of responding to congressional inquiry.

In the meantime, any agency that does not think it can provide the congressional offices with personal information is at liberty to gather information requested through the congressional office and forward it directly to the individual who is the subject of the record and request.

Congressional offices report that they have had few problems attributable directly to the Privacy Act in obtaining information from agencies since the implementation of the routine use regulation. Problems with the Immigration and Naturalization Service, Department of the Navy and other agency components have been quickly solved by referring agency officials to their own privacy regulations, or by conferring with privacy policy makers within the agencies.

I am referring copies of all agency responses to my survey to the OMB for support in asking all agencies to comply with the Oct. 3 guideline. Further, the Department of Justice has declared its support of the guideline and its intention to ask all agencies to comply should there be any agency that seeks to exclude itself from the government-wide policy.

One purpose of the Privacy Act of 1974 is to ensure that information collected by federal agencies will be used only for the purposes for which it was collected. The routine use does not enable congressional offices to collect information that has not been solicited by the subject of the information. Should any congressional office knowingly and willfully obtain a record on an individual from an agency under false pretenses, the person responsible in the congressional office is guilty of a misdemeanor and subject to a fine of up to $5,000.

63-619 O - 76 - 73

In January, my staff conducted a survey of congressional offices to discover how many are collecting evidence that a request from the constituent has been received. Such evidence--a letter, signature form or other authorization--is valuable for the congressional office to have in its files should the subject of any records request later claim he never made the request. Of course, under the OMB guideline as implemented by 31 agencies, this written evidence need not be presented to the agency concerned.

Sixty-nine representatives' presented over 90 different forms to the subcommittee. Several others always ask constituents to write a letter describing their difficulty. Many congressmen also make written requests to agencies about particularly sensitive cases. Only one office reported it never asks for something with the constituents signature attached.

The forms used range from simple mimeographed consent forms asking only the constituents signature to detailed forms asking the constituent to present his problem, supporting data and authorization to the congressional office in order to pursue his case with a particular agency. A few offices wisely note where the request was received, on what date and who handled the request.

I commend these offices for their desire to comply with the Privacy Act to the fullest and their initiative in determining that a requester is who he claims to be.

Facsimiles of several good forms will soon be available in the Congressional Handbook published by the Joint Committee on Congressional Operations.

The subcommittee will continue to monitor the constituent casework problem. Should any congressional office find an agency that is not complying with the OMB guideline, or its own regulation, I would appreciate having that information brought to my attention. Similarly, I hope federal agencies will apprise me of problems they encounter in implementing the regulation.

[illegible] JR., MICH.
TORBERT H. MACDONALD, MASS.
[illegible], CALIF.
MICHAEL HARRINGTON, MASS.
ANDREW MAGUIRE, N.J.
ANTHONY MOFFETT, CONN.

LAWRENCE J. BROWN, OHIO
PAUL N. MC CLOSKEY, JR., CALIF.
225-3741

NINETY-FOURTH CONGRESS

Congress of the United States

House of Representatives

GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS
SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS
RAYBURN HOUSE OFFICE BUILDING, ROOM B-349-B-C
WASHINGTON, D.C. 20515

December 22, 1975

Honorable Roderick Hills
Chairman
Securities and Exchange Commission
500 North Capitol Street
Washington, D. C. 20549

Dear Chairman Hills:

It has recently come to my attention that many agencies have not yet implemented the Office of Management and Budget guideline for the Privacy Act of 1974 regarding congressional inquiries on behalf of constituents. These agencies are not releasing information in response to telephone calls from congressional offices which affirm that a constituent request has, in fact, been received. In some cases, agencies are refusing to respond to inquiries even when the constituent's letter requesting help, or a form signed by the constituent authorizing the congressman to help, has been forwarded to the appropriate division within the agency.

When the Privacy Act became effective on September 27 of this year, this Subcommittee was overwhelmed with complaints from Members of Congress because executive agencies were refusing to deal with congressional inquiries and were citing the Privacy Act as the reason.

As a result of over a week of meetings between myself, congressional representatives, the OMB, and agency representatives, OMB Director James Lynn issued the following directive on October 3:

> Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

The guideline, a copy of which is enclosed, appeared in the Congressional Record of October 6, 1975, and the Federal Register of December 4, 1975.

Representatives of the Defense Department, the Veterans Administration, and the Department of Health, Education, and Welfare quickly assured me that their departments would amend their regulations to permit release of

a constituent's personal data to congressional offices upon telephonic assurance that the request for congressional help had been made by the constituent.

I am writing now to ask whether your agency is complying with the OMB guideline. As you may know, the guideline provides that if a constituent has asked for assistance, the Representative should inform the agency of that fact. The guideline does not require that the request be in writing, or that it be presented to the agency.

Please supply the Subcommittee with a copy of your agency's regulation implementing the OMB guideline. If you have not yet implemented the OMB language, please inform the Subcommittee of your reasons for not having done so.

Thank you for your prompt attention to this important matter.

Sincerely,

BELLA S. ABZUG
Chairwoman

cc: James Lynn, Director
Office of Management and Budget

Enclosure

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

COMPTROLLER
(Administration)

12 MAR 1976

MEMORANDUM FOR Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Director of Defense Research & Engineering
Assistant Secretaries of Defense
General Counsel
Director, Telecommunications and Command and Control Systems
Assistants to the Secretary of Defense
Directors of the Defense Agencies

SUBJECT: Defense Privacy Board Decision Memorandum 76-1

The purpose of this Decision Memorandum is to provide Privacy Board determinations regarding specific questions involving the Privacy Act - and in certain cases the Freedom of Information Act - to all Department of Defense Components for their information in implementing the Privacy Act of 1974 (P.L. 93-579, 5 U.S.C. 552a). The attached numbered determinations represent a compilation of various issues concerning the Privacy Act that have been presented for resolution to the Defense Privacy Board by Components. Only those determinations are included which appear to have commonality to all Components and as further Privacy Act questions are presented and resolved in the future, the additional determinations of general interest will be issued as a continuing series.

D. O. Cooke
Deputy Assistant Secretary of Defense

Attachments - 23

AMERICAN REVOLUTION BICENTENNIAL 1776-1976

PRIVACY ACT - PROVIDING WAGE AND EARNING STATEMENTS (W-2 FORMS) FOR MILITARY PERSONNEL TO STATE AND LOCAL TAX AUTHORITIES

The question presented is whether the Privacy Act permits the dissemination of wage and earning information on W-2 Forms to state, local and other taxing authorities. The information contained on W-2 Forms pertaining to members and employees is required to be disclosed to state and local taxing authorities under the Freedom of Information Act, 5 U.S.C. 552. No accounting of such disclosures is required. To the extent that the dissemination of such data could be considered an invasion of personal privacy, on the balance, any potential harm which may be suffered by a military member is far outweighed by the public interest in the dissemination of such data.

PRIVACY ACT - APPLICABILITY TO DECEASED PERSONS

The question presented is whether data concerning deceased service members/employees such as: dates of service, date and place of birth, date and geographical location of death, place of burial and service number, may be released under the Privacy Act.

The Privacy Act, as interpreted in the OMB guidelines of July 9, 1975, does not protect the records of deceased individuals from disclosure. Generally, in the case of decedents, this information may be disclosed. The Freedom of Information Act, however, authorizes withholding of some data to protect the privacy of next-of-kin in unusual circumstances not addressed here.

PRIVACY ACT - DISCLOSURE OF PERSONAL RECORDS OF PERSONS MISSING IN ACTION, OR OTHERWISE UNACCOUNTED FOR CONTAINED IN A SYSTEM OF RECORDS TO THEIR NEXT-OF-KIN

The question presented is what personal information relating to persons missing in action or otherwise unaccounted for may be disclosed under the Privacy Act. If a legal guardian has been appointed by a court of competent jurisdiction for a member who is missing in action or otherwise unaccounted for, then the guardian would be in the position of the member and have the same rights of access to records as the member would have. See 5 U.S.C. 552a(h). If a guardian has been appointed, personal records which are contained in a system of records and relate to the missing member should not be disclosed to other persons without the written consent of the guardian, unless disclosure is otherwise authorized by Section (b) 5 U.S.C. 552a. In those instances where no guardian has been appointed, only that information which is required to be disclosed under the Freedom of Information Act may be provided to a primary next-of-kin under the provisions of the Privacy Act. In determining exactly what information must be disclosed under the Freedom of Information Act, a balancing test which weighs the public interest of disclosure against the potential invasion of personal privacy must be made in each instance, which considers the particular circumstances of each case. Because the facts and needs will differ in each case, the balancing test may require disclosure of information in one circumstance but deny disclosure of the same information in another circumstance. See Getman v. NLRB, 450 F. 2d 670 (DC Cir 1971), app'l for stay of order denied, 404 U.S. 1204 (1971); Robles v. Environmental Protection Agency, 484 F. 2d 843 (4th Cir 1973); Wine Hobby, USA, Inc. v. United States Bureau of Alcohol, Tobacco and Firearms, 502 F.2d 133 (3rd Cir 1974). Each instance where personal information is requested must be considered on a case-by-case basis. Because of the unusual circumstances involved when a service member is missing in action or otherwise unaccounted for, considering the balancing of interests, the Freedom of Information Act would generally require disclosure of personal information to the next-of-kin of members missing in action. Although disclosure of personal information to next-of-kin would be required, it is believed that the interests of privacy would greatly outweigh the need to disclose this same information to other third parties. Hence, such information should not be disclosed to other than the next-of-kin unless specifically authorized under 5 U.S.C. 552a(b).

PRIVACY ACT - CORRECTIONS OF MILITARY RECORDS PERMITTED UNDER THE ACT

This addresses the question of when requests for correction of records should be processed under the Act and when an individual must go to the Board for Correction of Military or Naval Records. The question to be presented is whether 5 U.S.C. 552a(d)(2) permits an individual to request all corrections he believes warranted in his records, that are maintained in a system of records, under the Privacy Act. This question bears on the relationship of Privacy Act amendment process to the statutorily created Board for Correction of Military or Naval Records process. One of the main purposes of the Privacy Act was to insure that personal records relating to individuals were maintained accurately so that informed decisions based upon those records could be made. The Privacy Act amendment provision permits an individual to request factual amendments in his records which are maintained in a system of records. It does not ordinarily permit correction of judgmental decisions such as efficiency reports; selection and promotion board reports. These judgmental decisions should be challenged at the Board for the Correction of Military or Naval Records which by statute, 10 U.S.C. 1552, is authorized to make these determinations. While factual amendments may be sought under both the Privacy Act and the Board for Correction of Military or Naval Records, corrections other than factual matters ordinarily fall outside of the provisions of the Privacy Act and are in the purview of the Board for Correction of Military or Naval Records. If a factual matter is corrected under the Privacy Act procedures, any subsequent judgmental decisions that may have been affected by the factual correction, if contested, should be considered by the Board for the Correction of Military or Naval Records.

PRIVACY ACT - APPLICABILITY TO NATIONAL GUARD RECORDS

The question presented is whether the Privacy Act applies to records maintained by the National Guard. As used in the Privacy Act, "maintain" connotes the various records keeping functions to which the Act applies, i.e., maintaining, collecting, using, and disseminating as well as control over and hence the responsibility and accountability for systems of records (OMB Cir. No. A-108, 40 FR 28948, 28954 (1975)).

Section 275, title 10, United States Code, requires that each armed force maintain personnel records on each member of its reserve components. The reserve components of the Army and the Air Force include the Army and Air National Guards of the United States respectively, (10 U.S.C. 261), which are composed of federally recognized units and organizations of the Army or Air National Guard and members of the Army or Air National Guard who are also Reserves of the Army or Air Force respectively (10 U.S.C. 3077 and 8077). The mandate of section 275, title 10, United States Code, requires the Departments of the Army and the Air Force to maintain personnel records on all members of the federally recognized units and organizations of the Army and Air National Guards and on all members of the Army or Air National Guards who are also reserves of the Army and Air Force and are "maintained" by the Army or Air Force for the purposes of the Privacy Act. It is noted that these records are not all located at the National Guard Bureau. Some are located at the state and physically maintained by the state adjutant general. It is not, however, necessary that the records be physically located in the agency for them to be maintained by the agency (see OMB Cir. No. A-108, supra). The records located at the state level are under the direct control of the Army or Air Force in that they are maintained by the state as prescribed by regulations (NGR 600-200 and AFR 35-44) which implement section 275, title 10, United States Code, and are promulgated pursuant to the authority of the Secretaries of the Army and the Air Force (10 U.S.C. 280). These records are therefore, Army or Air Force records and subject to the provisions of the Privacy Act.

The determination that these records are subject to the Privacy Act does not mean that they cannot be used by the members of the state national guards unless such use is listed as a routine use and an accounting is kept. The state officials who use and maintain these records are members of the reserves (members of the Army or Air Force National Guard of the United States), and disclosure to them for the performance of their duties is a disclosure within the Department of Defense which does not require a routine use or an accounting.

PRIVACY ACT - FEE ASSESSMENT TO CONGRESSMEN FOR RECORDS FURNISHED WHICH ARE SUBJECT TO THE PRIVACY ACT

The question presented is whether members of Congress should be charged for records provided at their request under the guidance contained in DoD Directive 5400.11. Section (f)(5) of the Privacy Act states that each agency shall "establish fees to be charged, if any, to any individual for making copies of his record...". OMB guidance and DoD Directive 5400.11 both point out that if a fee is charged, only the direct cost of making the copy may be collected. This guidance also states that if copying is the only means whereby the record can be made available to the individual, reproduction fees will not be assessed.

Therefore, the charging of a fee is a discretionary matter on the part of the agency. In view of this, it is proposed that from a policy standpoint, DoD not charge Congressmen for records furnished when requested under the Privacy Act, unless the charge would be substantial. In no event should a fee below $25.00 be determined substantial. It is recommended that in constituent inquiries where the fee is substantial, a suggestion should be made that the Congressman advise his constituent that the information may be obtained by writing the appropriate office and payment of the cost of reproduction. Additionally, the record may be examined at no cost if the constituent wishes to visit the custodian of the record.

PRIVACY ACT - RELEASE OF HOME OF RECORD TO MEMBERS OF CONGRESS

The question presented is the propriety under the Privacy Act of 1974 (5 U.S.C. 552a), of releasing a service member's "home of record" from his service record to an inquiring Member of Congress or Congressional staff member. The new routine use provisions for DoD Systems of Records published on 9 October 1975 (40 FR 47748) which became effective on 8 November 1975 are sufficiently broad to permit the release of home of record information to a Member of Congress or Congressional staff member who is making an inquiry of a DoD Component at the request of the subject service member, even if the subject member's request did not concern that particular portion of the service record.

It should be noted, however, that the service record entry for home of record is intended only to reflect the service member's home at the time of entry into the service or call to active duty. It may not reflect the member's current legal residence or domicile for voting purposes, and the Member of Congress or Congressional staff member may be more interested in the subject service member's legal residence as entered on a W-4 form by the service member and as reflected by the member's pay record. Any release of home of record information to a Member of Congress or to a Congressional staff member should be caveated with the notation that it only reflects the home address at the time of entry into the service or call to active duty.

PRIVACY ACT - DISCLOSURE ACCOUNTING FOR RECORDS DISCLOSED THROUGH MILITARY LEGISLATIVE LIAISON CHANNELS

The question presented is what procedures and divisions of responsibility should be established by military departments to ensure the preparation of required disclosure accountings where information concerning individuals is disclosed to Members of Congress through departmental legislative liaison channels from records maintained by other activities, with the consent of the individuals concerned, pursuant to the newly effective DoD "routine use." It is noted that, under subsection (c) of the Privacy Act of 1974 (5 U.S.C. 552a) disclosure accountings apparently are required in instances of consensual disclosures and disclosures made pursuant to subsection (b)(3).

Where a disclosure is made directly to a Member of Congress by an activity having custody of the record that is disclosed, no substantial question exists under present DoD policy as to that activity's responsibility for maintaining an appropriate record of the disclosure for future accounting purposes in accordance with that activity's procedures implementing the Privacy Act. A more difficult administrative problem arises, however, where the requested information is transmitted by the custodial activity to the legislative liaison activity for retransmittal -- possibly in a form that deletes some data furnished by the custodial activity, or that consolidates the information with information from records in the custody of other activities -- to the requesting Member of Congress. In the latter situation, it might frequently be impossible for the custodial activity to discharge the systems manager's responsibility of compiling and maintaining an accurate record of what was actually disclosed to the requesting Congressional office unless the custodial activity receives feedback from the legislative liaison.

It is questionable whether an attempt should be made to resolve the problem on a DoD-wide scale, because the formulation of specific procedures and responsibilities in connection with maintaining records required for disclosure accounting purposes apparently will involve consideration of a number of factors which will vary among the different military departments and other DoD Components, such as internal organizational relationships, a Component's prescribed methods and responsibilities for responding to Congressional inquiries and possibly the characteristics of the particular records and record systems involved.

It is recommended that the liaison activity prepare a disclosure accounting to be maintained by the custodial activity. In each case where information is disclosed as a routine use, a record of disclosure should be made and maintained for five years or the life of the record, whichever is longer. Therefore the discloser of the information should make a record of disclosure

which contains, as a minimum, the name, rank, grade or rating, social security number of the person from whose record disclosure is made; the date, nature and purpose of the disclosure; and the name of the person to whom the disclosure is made, and the Member of Congress for whom he works. The name, rank, grade or rating, duty station, and where applicable, office title of the person making the disclosure should also be included. This record of disclosure should then be forwarded to the person who maintains the record from which the disclosure is made, or such activity as is designated by competent authority.

PRIVACY ACT - DEFINITION OF A "MINOR"

The question presented is who is a "minor" for purposes of the Privacy Act. The Privacy Act provides that the parent of any minor may act on behalf of that individual. OMB guidelines stress that this provision is in the alternative and permissive and thereby not construed as limiting the minor's right to access.

Under common law, a minor is a male or female child under 21. This definition is generally accepted unless modified by state law or unless the minor is emancipated by agreement between the parent and child, by enlistment in the military, by marriage, or by court order. In the view of the Privacy Board, the determination of minority would normally be dependent upon the state law where the minor is located. Determination therefore must be made on a case by case basis. In making these determinations, close attention should be given to the growing body of law allowing minors to make medical decisions about themselves without parental consent and the implied or express right of privacy of the minor contained therein.

Members of the armed forces are considered emancipated for purposes of the Privacy Act.

PRIVACY ACT - THE USE OF INFORMATION FROM CONFIDENTIAL SOURCES BY INVESTIGATIVE ACTIVITIES IN RELATION TO OMB GUIDELINES

The question presented is whether the OMB guidance on section (k)(2) of the Privacy Act requires disclosure of a confidential source if the individual concerned was denied a right, benefit or privilege as a result of the information received. Normally, investigative activities will list interviewees, companies, firms or agencies as confidential sources in reports of investigation when the releasor of the information specifically requests confidentiality as a condition precedent to providing the information.

Subsection (k)(2) of the Office of Management and Budget (OMB) Privacy Act Implementation Guidelines states, in part, the following concerning confidential source information:

"Furthermore, the acceptance of this section in no way precludes an individual from knowing the substance and source of confidential information, should that information be used to deny him a promotion in a government job, or access to classified information or some other right, benefit, or privilege for which he was entitled to bring legal action when the government wished to base any part of its legal case on that information." (emphasis supplied)

Investigative activities are concerned about the possibility of an individual requestor taking adverse action based upon confidential source information in the report of investigation which could result in having to divulge the identity of the confidential source.

That portion of the quoted OMB language relating to an individual "... knowing the substance and source of confidential information..." appears to be in direct conflict with all of the preceding language of subsection (k)(2) of the guidelines, which provides very clearly for withholding the identity of a source in a proper case. OMB was queried concerning this apparent conflict and advised that the quoted section of Senator Ervin's statement relates not to the administrative process of declining to identify a source pursuant to to subsection (k)(2) of the Act, but to the requestor's judicial remedies afforded by the Discovery Rules and subsection (g)(3)(A) of the Act.

In view of the foregoing, no objection is perceived as to the current administrative procedures of investigative activities of utilizing confidential sources in reports of investigations, which appear to be consistent with the Privacy Act and the OMB guidelines.

63-619 O - 76 - 74

PRIVACY ACT - APPLICATION OF ACT TO INFORMATION FROM HOSPITAL COMMITTEE MINUTES

The question presented is whether hospital committee minutes must be provided to patients or physicians under the Privacy Act. Hospital committee minutes such as medical audit, tissue, utilization, medical records and credentials, are not filed and indexed under the name or identifying number of the patient or physician. These minutes are not systems of records which are subject to the requirements of the Privacy Act. Therefore, access to these minutes need not be granted to the patient/physician under the Privacy Act.

PRIVACY ACT - ACCOUNTING FOR MASS DISCLOSURES OF PERSONAL INFORMATION TO OTHER AGENCIES

The question presented is whether inter-agency support agreements could be negotiated which would negate the requirement to account where "mass" disclosures are made to other specific agencies such as GAO. 5 U.S.C. 552a(c) requires that, except for intra-agency disclosures made pursuant to the Freedom of Information Act (FOIA), each agency keep an accurate accounting of all disclosures made from systems of records under its control. Generally, mass disclosures made to other government agencies fall under this requirement and an accounting is required.

Neither the Act nor OMB guidelines, however, specify a form for maintaining this accounting. They require only that an accounting be maintained, that the accounting be available to the individual named in the record and for use to advise of corrections of records and that it be maintained in such a way that a disclosure of records may be traced to the records disclosed. Specific records need not be marked to reflect disclosure unless necessary to satisfy this tracing requirement.

Accordingly, with respect to mass disclosure, if the disclosure is of all records or all of a category of records or of records released at the request of the individuals, e.g., with transmittal of payroll checks to banks, it should be satisfactory simply to identify the category of records disclosed including the other information required under 5 U.S.C. 552a(c) on some comprehensible form and make that form available, as necessary, to satisfy the accounting of disclosure provisions of the Act. Similarly, if the disclosures occur at fixed intervals, a statement to this effect, as opposed to a statement at each occasion of release, should satisfy the accounting requirement. If the mass disclosure is not of a complete category of records but, for example, a random selection within a category, then the above information with a list of the individuals' records disclosed could be maintained. Appropriate officials could then review this list, as necessary, to provide information to satisfy the accounting provisions of the Act.

It is not deemed appropriate to enter into inter-support agreements with the General Accounting Office (GAO) since they are not an executive agency and the requirement to account for disclosure to GAO is specifically provided for in the Privacy Act. However, inter-agency support agreements may be entered with other executive agencies as specified in DoD Directive 4000.19 and authorized by the OMB guidelines.

PRIVACY ACT - RELEASE OF PERSONAL INFORMATION TO STATE AGENCIES TO VALIDATE UNEMPLOYMENT COMPENSATION CLAIMS OF FORMER FEDERAL EMPLOYEES AND MILITARY MEMBERS

The question presented is the propriety under the Privacy Act of 1974 (5 U.S.C. 552a) of releasing information from employment or service records as required by 5 U.S.C. 8506 and 8523 to State agencies administering unemployment compensation claims. The latter two sections require Federal agencies, under specified circumstances, to provide to appropriate State agencies personal information, including the period of Federal or military service, if any, the pay grade or amount of Federal wages and allowances, the reasons for termination of Federal service or discharge from military service, and the conditions under which a military discharge or resignation occurred.

Portions of the required information may be released to any requestor pursuant to the Freedom of Information Act and subsection (b)(2) of the Privacy Act of 1974, such as the period of Federal or military service and the pay grade and amount of wages and allowances received (see subparagraph B.2. of enclosure 5 of DoD Directive 5400.11 of August 4, 1975, Subj: Personal Privacy and Rights of Individuals Regarding Their Personal Records). Information concerning the reasons for termination or discharge and the conditions of discharge could only be released pursuant to the advance written consent of the subject individual provided by the State agency under subsection (b) of the Privacy Act of 1974, or pursuant to a routine use established for the appropriate systems of records pursuant to subsections (b)(3), (e)(4)(D) and (e)(11) of the Privacy Act of 1974. It should be noted that DoD Components have published routine uses of personal records systems which are sufficient to permit this disclosure.

Likewise, the routine use provisions of the Civil Service Commission System Notice for "General Personnel Records---CSC" published on 27 August 1975 (40 FR 39245) contain the following statement, "Information in these systems is used or may be used . . . (for disclosure to a) state, county (or) municipal, or other publicly recognized agency of information needed to adjudicate a claim for benefits under the BRIOH or the recipient's benefit program . . ."

PRIVACY ACT - RELEASE OF GEOGRAPHICAL LOCATION OF PLACE OF DUTY

The question presented is whether the geographical location of an individual's place of assignment may be disclosed under the Privacy Act. DoD Directive 5400.11 provides that certain personal information is releasable without an unwarranted invasion of privacy, examples include: "salary, present and past duty assignments, future assignments which have been finalized, office phone numbers..." Civilian employees of the Military Departments are subject to the release of their office address under the same directive, as provided by the Federal Personnel Manual. "Duty assignment" of current directives is interpreted to include: office address, duty station address and geographical location. Therefore, a request under the Freedom of Information Act for information about the geographical location of assignments is releasable unless classified.

PRIVACY ACT - RELEASE OF INFORMATION CONTAINED IN MILITARY PERSONNEL RECORDS

The question presented is what information from personnel records is releasable to the public.

Decedents: The definition of the term "individual" in the Privacy Act clearly implies that the status only applies to living persons.

Age (Date of Birth): Generally releasable under the FOIA exception (6). There is little to commend an argument that releasing this data would constitute an unwarranted invasion of privacy. Public records pertaining to age are legion, including officer lineal listings. It has been traditional practice to release this information in news stories.

Home of Record: No general rule for the disclosure of an individual's home of record can be adopted because of the wide differing circumstances that are present in requests for this item of information. As the facts and needs will differ in each particular circumstance, a balancing test must be made on a case by case basis. See Getman v. NLRB, 450 F. 2d 670 (D.C. Cir 1971), app'l for stay of order denied, 404 U.S. 1204 (1971); Robles v. Environmental Protection Agency, 484 F. 2d 843 (4th Cir 1973); Wine Hobby, USA, Inc. v. United States Bureau of Alcohol, Tobacco & Firearms, 502 F. 2d 133 (3rd Cir 1974). However, home of record may usually be released if no street address is given. In most cases, in response to questions, an individual's present geographical location, i.e., Cleveland, Ohio, may be provided but not the individual's street address. The street address may not be released without individual consent or a determination of overriding public interest.

Whenever feasible, the desires of the individual or next-of-kin with regard to disclosure of the home of record should be ascertained and considered. In many instances consent to release may be obtained thus obviating the problem. However, the desires of the individual or next-of-kin are not necessarily controlling and when an objection to release is made, a balancing of interests under the FOIA may still require disclosure.

Marital Status: i.e. married or not married, is disclosable as it is a matter of public record and is disclosable under FOIA.

Dependents: Names, sex, age and number of dependents may be disclosed under FOIA.

Awards and Decorations: Generally releasable under the FOIA exception or source other than official record. The presentation of an award or decoration is generally a public event, usually the subject of some publicity in the local facility newspaper, and in the case of many awards and decorations

there is a visible token thereof worn upon the uniform. There is simply no basis to claim an unwarranted invasion of privacy.

Education/Schooling: Generally releasable under FOIA exception. DoD Directive 5400.11 provides in paragraph B. 2., enclosure 5, that such information may be released. Information as to the major area of study, school, year of graduation and degree are generally releasable under the FOIA.

Race: To release information departmental records regarding race may constitute an unwarranted invasion of privacy. While the relevance of rac to a news story appears to be questionable, and routinely providing such information would appear to be questionable as a matter of sound policy, it is recognized that on occasion a specific request may be made for such information in circumstances in which it is relevant - - e.g., a racially oriented protest or altercation. If it is essential to respond to a media query and the information may be obtained from sources (racial categories often are discernible upon sight) other than official records, there would appear to be no legal prohibition to its release.

Character of Discharge: In the case of discharges resulting from administrative processing, the character of discharge is not a matter of public record, and the procedures and/or hearing leading to discharge are not public. The Department of Defense has gone to great lengths to preserve the confidentiality of the character of discharge - - e.g., removal of SPN numbers from the DD-214. The release of this information to the general public has thus been viewed as an unwarranted invasion of privacy and not releasable under the Privacy Act unless the individual provides his written consent. In the case of discharges premised under courts-martial, the proceedings and record are exempt from the restrictions of the Privacy Act by virtue of the fact that the Act incorporates the definition of "agency" found at 5 U.S.C. 551(1) which specifically excludes courts-martial (see 5 U.S.C. 551(1)(f)). The proceedings are public. Therefore, the approved sentence and subsequent clemency action, if any, are releasable under the FOIA.

Duty Status at a Given Period of Time: This is releasable under the FOIA exception. Paragraph B.2. enclosure 5, DoD Directive 5400.11, specifically permits the release of information regarding duty status as specified in appropriate Component directives. Release of information such as the fact of unauthorized absence/desertion, hospitalization, in hands of civil authorities awaiting trial, and confinement by military authorities awaiting trial is permitted. When an individual is hospitalized, it is permissable to disclose his general condition, i.e., critically ill, good condition, etc.

Decisions of Personnel Boards (release after decision by highest authority): Releasable under FOIA exception, if the board action applies to a category of persons, as opposed to an individual. Otherwise unreleasable. There are a myriad of personnel board actions which are accomplished each year. Some affect

groups of persons, e.g., promotion boards, augmentation boards, others affect individuals, e.g., administrative discharge boards, aviator flight boards. Results of the former group have traditionally been released to the press. DoD Directive 5400.11 implicitly recognizes the public nature of such boards by including promotions and by analogy other similar board actions as being a matter within the public domain and releasable. See paragraph B.2. of enclosure 5. The results of the latter category of boards have not been traditionally released, the board proceedings are not public, and the nature of the action taken, often adverse, warrants preservation of its confidentiality. Information may be confirmed which has become a matter of public knowledge by the action of the individual or his counsel.

PRIVACY ACT - PROVIDING INFORMATION ON FEDERAL EMPLOYEES AND MILITARY MEMBERS TO FINANCIAL INSTITUTIONS

What information may be provided concerning Federal employees and military members in response to a credit investigation inquiry by a credit bureau or other representative of the credit granting industry?

Subparagraph B.2. of enclosure 5 of DoD Directive 5400.11 of August 4, 1975, Subj: Personal Privacy and Rights of Individuals Regarding Their Personal Records, provides that information concerning a military member's rank, date of rank, salary, present and past duty assignments, future assignments which have been finalized, office phone number, and office address may be provided to any member of the public pursuant to the Freedom of Information Act (5 U.S.C. 552) and subsection (b)(2) of the Privacy Act. This information as well as other similar information such as the member's length of military service and duty status may be provided by any DoD activity unless the information has been classified in the interest of national defense or foreign policy.

It is further noted in this regard that subchapter 7 of chapter 294 of the Federal Personnel Manual authorizes the release of information concerning a Federal civilian employee's present and past position titles, grades, salaries, and duty stations (including office address) to the public if the information is not classified and is not being sought for political or commercial solicitation purposes. The cited subchapter further provides that credit firms may be provided more detailed information concerning tenure of employment, Civil Service status, length of service in the agency and the Federal Government, and certain information concerning the separation of an employee. It is considered that the Federal Personnel Manual provisions are consistent with the provisions of the Privacy Act and Freedom of Information Act in this regard.

Where release of particular information requested by a credit bureau would not be authorized under the provisions described above, any personal information may be disclosed from military or civilian personnel records by DoD Components, pursuant to subsection (b) of the Privacy Act, when there is written consent of the subject employee or military member specifically authorizing the release of the requested information.

See also a notice concerning Military Banking Facilities in the Federal Register of 13 February 1976 (41 FR 6779).

PRIVACY ACT - DISCLOSURE OF PHOTOGRAPHS IN THE CUSTODY OF THE DEPARTMENT OF DEFENSE

The question presented is whether official photographs in the custody of the Department of Defense may be released to the public and if a Privacy Act advice must be given when a photograph is taken. Photographs taken for official purposes of members of the armed forces and DoD employees are generally releasable under the Freedom of Information Act, 5 U.S.C. 552a(b)(2) unless the photograph depicts matters that if disclosed to public view would constitute a clearly unwarranted invasion of personal privacy. Generally, award ceremony photographs, selection file photographs, chain of command photographs and similar photographs are releasable. When such photographs are taken, it is not the collection of information contemplated by section (e)(3) of the Privacy Act and no Privacy Act advice is required.

PRIVACY ACT - DISCLOSURE OF RECORDS FROM SYSTEMS OF RECORDS TO A CONTRACTOR PURSUANT TO A CONTRACT

The question presented is whether disclosure of personal records from a system of records to a contractor for the performance of a contract may be disclosed under section (b)(1) of the Privacy Act. The disclosure of records from systems of records to a contractor pursuant to sections 3(b)(1) and 3(m) of the Privacy Act requires neither consent of the individual nor maintenance of a disclosure accounting record.

Section 3(m) of the Privacy Act, as interpreted by the Office of Management and Budget implementation guidelines (Federal Register, Volume 40, Number 132, pages 28975-28976) sets forth the necessary guidance in this matter. It provides that a system of records operated under contract to accomplish an agency function, is in effect deemed to be maintained by the agency. Under these guidelines, disclosures of personal information between an agency and its contractors fall under subsection 3(b)(1) of the Act, i.e., "to those officers and employees of the agency which maintains the record who have a need for the resord in the performance of their duties." The Privacy Act does not impede disclosure of information to a contractor and system notices do not require any change to reflect use by a contractor.

PRIVACY ACT - APPLICATION OF LAW ENFORCEMENT PROVISIONS TO STATE AND LOCAL PROBATION, PAROLE OFFICERS, PENAL, MENTAL, AND/OR CORRECTIONAL INSTITUTIONS UNDER THE PRIVACY ACT

The question presented is whether state and local penal, mental and correctional institutions as well as probation and parole officers are law enforcement agencies within the provisions of the Privacy Act. Criminal law enforcement agencies and criminal justice means any activity pertaining to crime prevention, control or reduction, or the enforcement of the criminal law, including, but not limited to police efforts to prevent, control, or reduce crime or to apprehend criminals, activities of courts having criminal jurisdictions and related agencies (including prosecutorial and defender service), activities of correctional, probation, or parole authorities, and programs relating to the prevention, control, or reduction of juvenile delinquency or narcotic addiction.

Criminal law enforcement agencies are those local, state, or federal agencies thereof, such as those described above, including probation officers, which perform the administration of criminal justice pursuant to lawful authority.

PRIVACY ACT - FORMAT FOR PRIVACY ACT STATEMENTS

The question presented is what format should be followed in printing Privacy Act statements. The placement of the Privacy Act statement in a form should be in the following order of precedence:

1. Enclosed in the body of the form, preferably below the title and positioned in such a manner that the individual will be advised of the information required by the Act, or a statement showing the location of this information before he begins to furnish any of the information requested.

2. Placed on the reverse of the form with an appropriate notation under the title of its location.

3. Attached to the form as a tear-off sheet.

4. Issued as a separate supplement to the form.

PRIVACY ACT - PRIVACY ACT STATEMENTS FOR INSPECTOR GENERAL COMPLAINT FORMS

The question presented is whether or not a Privacy Act advice (5 U.S.C. 552a, (e)(3)) is required for Inspector General Complaint forms. This question arises because the Component does not initiate a request for information from the individual, but only asks for certain information in order to respond to a complaint which was voluntarily initiated by the individual himself. The initiation of a course of action by the voluntary action of an individual does not preclude theneed for a Privacy Act statement. The purpose of providing a Privacy Act statement is the notion of informed consent since an individual should be provided with sufficient information about the request for information so he may make an informed decision as to whether or not to respond. See OMB Guidelines, (40 FR 28961), dated July 9, 1975. The intent of the Privacy Act is to, in all instances, advise individuals whenever they are requested to provide personal information as to the authority for collection of the information, the uses to be made of the information, whether it is voluntary or mandatory to provide the information, and the consequences of not providing the information. Whenever a Component asks for information, a Privacy Act statement must be provided. We perceive no difference between an Inspector General complaint which triggers a request for information and medical forms which are completed only after the individual voluntarily initiates a request for treatment. It has been determined by all agencies that all medical forms require a Privacy Act advice.

PRIVACY ACT - RECRUITMENT ADVERTISEMENTS IN THE PUBLIC MEDIA

The question presented is whether recruitment advertisements in newspapers, etc., requires the publishing of a Privacy Act statement if a mail in coupon is provided for those individuals who desire further information.

Insofar as the published coupons and business return postcards merely provide the individual a vehicle with which he can request information from the military service concerning a particular recruiting program, no Privacy Act statement is required, as the service has not solicited information from the individual up to that point. The coupon or postcard used as a vehicle for the individual's solicitation of the service could include blanks for the individual's name, address, phone number, and other blocks for the individual to indicate his interest in a particular program and/or to provide information regarding his or her eligibility for a particular program (i.e., age, education level and sex). The individual's SSN does not appear to serve a significant purpose in the process of providing appropriate information to interested persons. If it is necessary for internal accounting purposes to include a blank for the individual's SSN, then a Privacy Act statement similar to the one below would be sufficient if it reflects the uses to be made of the SSN.

"We will be happy to provide you more information about the Army opportunities as authorized by 10 U.S.C. 503. The information voluntarily submitted, including your social security number, will be used for recruiting purpose. Failure to provide sufficient information may preclude action on your inquiry."

PRIVACY ACT - REQUIREMENT FOR PRIVACY ACT STATEMENT WHEN INFORMATION REQUESTED IS IN PUBLIC DOMAIN

The question presented is whether the Privacy Act advice specified under section (3)(3) of the act must be given when the only information sought must be disclosed under the FOIA. Paragraph B, enlcosure 6, DoD Directive 5400.11 requires that Privacy Act advice be given whenever an individual is requested to supply personal information. The Privacy Act requirement, 5 U.S.C. 552a (e)(3), is not necessary when the only information requested is that which is required to be disclosed by the FOIA, providing the disclosure of such information does not inferentially disclose other personal information not releasable under the FOIA. Examples of such information are, but not limited to, name, grade, organization, duty assignment, and official telephone number.

[From the Congressional Record—Senate, Oct. 9, 1975]

FREEDOM OF INFORMATION AND THE PRIVACY ACT

Mr. KENNEDY. Mr. President, last fall Congress enacted two bills designed to have a significant impact on the Federal Government's handling of information: the Privacy Act, and the Freedom of Information Amendments of 1974. The Privacy Act created a right of access for individuals to their own files, a right to correct mistakes contained in those files, and a responsibility on the part of the Government to protect personal information from misuse and disclosure which constituted an invasion of the privacy of the subject of that information. The Freedom of Information Act amendments speeded access by the public to Government records, strengthened the rights of the public to obtain disclosure of public information and limited the scope of the Government's authority to withhold certain kinds of information.

Both of these laws serve important and coordinate purposes. They help the public obtain ready access to information which should be available; and they guard against disclosure of information which should not be made public. These laws are not conflicting in intent or purpose. The Freedom of Information Act had always recognized the Government's authority to withhold information whose disclosure would constitute a clearly unwarranted invasion of personal privacy. And the Privacy Act was drafted to avoid interference with the free flow of information to the public required to be released by the Freedom of Information Act. They were enacted but a few weeks apart by a Congress dedicated both to an opening of the Federal Government—so recently tainted by the effects of the Watergate scandal—and to a protecting of the rights to personal privacy of each citizen who became the subject of a government file.

Nonetheless, with the need to enact the Freedom of Information Act amendments over the veto of President Ford, and with the need to complete work on the Privacy Act in the closing days of the 93d Congress, the two laws do not appear to mesh as easily as might have been desired. Two different committees in the Senate worked on the different bills; and while the Office of Management and Budget was pressing hard for enactment of privacy legislation, the Justice Department was pressing equally hard to defeat of Freedom of Information legislation.

On September 27 the Privacy Act became effective, and it is thus now necessary for agencies to determine how they will treat problems arising where that law and the Freedom of Information Act interface. In resolving these problems, the Justice Department and the Office of Management and Budget play central roles. For the Information Act recognizes that Justice must play a leadership role in insuring agency implementation of that act, while the Privacy Act places OMB in the leadership position. The Justice Department's legal advice is still crucial under the Privacy Act, since Justice must defend any litigation arising under that law.

Mr. President, the Justice Department got off to a rather disquieting start when on July 30 it sent out a letter advising the general counsel of one agency that the Privacy Act impliedly repealed cer-

tain disclosure requirements of the Freedom of Information Act. In the Department's view, according to the letter signed by a Deputy Assistant Attorney General, the Privacy Act was "exclusively applicable to all records in which an individual requests records from a system of records covered by" that act. This meant that an agency decision to exempt systems of records from public access under the Privacy Act also exempted them from disclosure under the Freedom of Information Act—a conclusion unsupported by the language of the laws or the intent of Congress, in my view. I will insert this letter in the Record at the end of my remarks as exhibit 1.

I wrote the Attorney General requesting his review of this matter, suggesting that the preliminary conclusion by Justice "could prove pernicious and destructive if allowed to become the official Justice Department interpretation of the law." (See exhibit 2.) I pointed out that the logical implications of the earlier position would mean a third party would have more rights than the subject of a file, and that the language of the Privacy Act appeared clearly to recognize the continued application of the full force of the Freedom of Information Act wherever the Privacy Act did not apply. I observed:

> It appears clearly intended that access under the Privacy Act is to be complete, and not subject to FOIA exemptions, where the Privacy Act grants access. But where the Privacy Act does not grant access, the FOIA—and its exemptions—apply.

I subsequently sent the Attorney General a Library of Congress analysis I had requested, which examined in great detail the Department's initial conclusion on this issue. That analysis concluded, as I had, that the Privacy Act is not an exclusive means of gaining access to personal information contained in a system of records:

> It flies in the face of the whole legislative effort in this area to construe the Privacy Act as a backhanded method to limit individual access to records while at the same time preserving potentially greater access rights to third parties.

The Library of Congress study is included below as exhibit 3.

Last week I received a response to my letter, from Deputy Attorney General Harold Tyler. (Exhibit 4.) Mr. Tyler indicated that he and others at Justice shared my concern, and he proposed that an amendment to the Department's privacy regulations would respond adequately to that concern. They respond, but clearly not adequately.

Mr. President, the Justice Department, in its proposed new regulation, meets the most important element of my objections: it provides as a practical matter that records exempted from application of the Privacy Act will nevertheless be available to a requester if he would otherwise have been entitled to them under the Freedom of Information Act. "To the extent that the individual seeks access to records from systems of records which have been exempted from the provisions of the Privacy Act," reads section 16.57(b) of the proposed new regulation,

> The individual shall receive, in addition to access to those records he is entitled to receive under the Privacy Act and as a matter of discretion . . ., access to all records within the scope of his request to which he would have been entitled under the Freedom of Information Act . . . but for the enactment of the Privacy Act and the exemption of the pertinent systems of records pursuant thereto.

This resolution of the issue effectively guarantees, at least temporarily, the substantive access rights provided the public under the Freedom of Information Act. But that is precisely what the law requires. The Department's action therefore falls short, in three ways, of complying with the letter and spirit of the Freedom of Information Act.

First, Justice has decided to grant access consistent with the Freedom of Information Act only as a matter of agency discretion—as a matter of grace. It seems thereby to try to duck resolution of the issue squarely as being mandated by the law. The Information Act in 1966 was passed with a primary objective of removing Government secrecy from the realm of official discretion for the most part; the only information which could be withheld was to be that "specifically" authorized by the act to be withheld. The law says:

> This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated.

Courts subsequently held that they had no discretion to allow the withholding of information required to be disclosed by the act, even under their traditional equitable powers. But now the Justice Department, though agreeing that the Privacy Act does not curtail the public's rights under the Freedom of Information Act, says that it is carrying out this conclusion "at the sole discretion of the Deputy Attorney General." Under this approach the next Deputy Attorney General might change his mind.

Second, because of its resolution of this issue as a matter of grace rather than law, the Justice Department has abrogated its general responsibilities as lawyer for the executive branches and its specific duty under the Information Act to "encourage agency compliance with" the act. It has now told another agency, last July, that the agency can refuse access required by the Freedom of Information Act, though at the same time it is saying that the Department itself would never do such a thing. While it may be hoped that the Office of Management and Budget will live up to its role in guiding the agencies on their duties under the law, I would urge Justice itself to provide more persuasive guidance to the agencies. After all the Justice Department will be defending those agencies in court, and I am all too confident it will lose its case in defending any agency that chooses—in exercising its discretion—to take what Justice leaves open as an alternative route for handling information requests.

Third, the Department has chosen to handle requests under privacy procedures, though it recognizes the need to apply Freedom of Information substantive standards. This deprives the requester of a timely response—within 10 working days—and other procedural benefits conferred by the Freedom of Information Act. I am well aware of the more direct conflicts between the two laws on questions of procedure. But it seems to me that where records have been exempted from disclosure under the Privacy Act, but remain subject to mandatory disclosure under the Freedom of Information Act, the procedures of the latter law should govern.

Mr. President, there has already been substantial litigation under the Freedom of Information Act. Over the past few weeks I have placed in the Record lengthy lists of cases pending and decided under that act. I think that agencies must do all that they can to avoid

litigation, and I would not encourage the public to resort to the courts where patience and perseverance can bring results at the agency level. So while I believe the Justice Department has reached the right results in deciding to release information concurrently under the Privacy and Information Acts, the manner in which it has done so borders on the irresponsible—and it is bound to cause additional litigation involving the hundreds of other agencies of government who may be going their own way.

The Privacy Act has its purposes and objectives. The Freedom of Information Act also has its own. The two sets of purposes and objectives are entirely consistent and complementary. It is the responsibility of the agencies to work out procedures which are likewise. For Congress is committed to a responsible, accountable, and open government, as well as to protection of personal privacy by the Government. The Freedom of Information Act and the Privacy Act strike the balance. It is up to the Government agencies who administer those laws to maintain it.

I ask unanimous consent that the documents referred to above be printed in the Record.

There being no objection, the documents were ordered to be printed in the Record, as follows:

EXHIBIT 1

JULY 30, 1975.

MEADE WHITAKER, Esq.,
Chief Counsel, Internal Revenue Service,
Washington, D.C.

DEAR MR. WHITAKER: In a letter dated April 14, 1975, Harold T. Flanagan, Director of your Disclosure Division, requested our views as to whether the Privacy Act of 1974, P.L. 93-579, is the exclusive avenue available to an individual who seeks government records about himself, or whether the Freedom of Information Act would also be available for this purpose.

Neither the literal language of the two Acts nor their legislative histories provide a clear answer to this question. The Freedom of Information Act provides that government records are available to "any person" who requests them unless they fit into one of nine exempt categories, in which case the agency may, but need not, refuse disclosure. The Privacy Act authorizes "an individual" to request records pertaining to himself and seek correction of those records, subject to two general and seven specific exemptions. The Freedom of Information Act, having been passed and amended first, makes no reference to the Privacy Act. The Privacy Act makes only two direct references to the Freedom of Information Act. New section 5 U.S.C. 552a(b)(2) permits disclosure of records about an individual without his prior consent if disclosure would be *required* by the Freedom of Information Act. Subsection (q) of the same section specifies that an agency may not use a Freedom of Information Act exemption to deny an individual access to files about him that would be available under the Privacy Act. No mention is made of the possibility that an individual might seek records under both Acts.

It should be noted that an earlier version of the privacy bills did address this question. Section 205(b) of H.R. 16373, as it passed the Senate on November 22, 1974, specified:

"Nothing in this Act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder."

This language would have assured that information available under the Freedom of Information Act would continue to be available, to the individual as well as to third parties, despite any broader exemption in the Privacy Act. The omission of this language from the final enactment suggests that Congress ultimately decided that the Privacy Act exemptions should govern exclusively, although the omission is not explained in the legislative history of the version that finally passed.

Since no clear reason is given for the omission of this language in the legislative history, it might be argued that the two Acts were nevertheless intended to provide alternate or duplicate remedies for an individual who seeks access to records about himself. In our view, however, a reading of the two Acts as a whole and consideration of their practical application leads to a contrary conclusion, namely, that the Privacy Act is the exclusive remedy for an individual who seeks records about himself contained in a system of records covered by the Privacy Act.

ALTERNATIVE APPLICATION

There would be no difficulty in harmonizing application of the two Acts to the same request if the effect of the Privacy Act were merely to expand access which the FOI Act already provides. Then one might reasonably assert that a requester was free to proceed under the older legislation—but could obtain still more by proceeding under the newer. It is true that in most respects the Privacy Act expands access by the person seeking his own records; but in sevral significant respects, the Privacy Act also permits or requires limitations upon access, beyond what the FOI Act would authorize.

For example, under the FOI Act an Agency could provide personal files to a person claiming to be their subject without requiring him to produce solid proof of his identify; subsection (f)(2) of the Privacy Act, however, authorizes the establishment of verification procedures. Similarly, under the FOI Act an agency would not be able to withhold medical information from its subject merely because it determined that disclosure would be harmful to him; whereas subsection (f)(3) of the Privacy Act permits an agency to restrict certain disclosures to the requesting subject's physician rather than making them to the subject himself. Finally, mention might be made of the Privacy Act's prohibition on access to information compiled in anticipation of a civil proceeding. Subsection (d)(5). It is entirely implausible that such substantial protections as these were intended only to apply to the incremental access which the Privacy Act provides beyond that of the FOI Act—so that they could be entirely avoided if the FOI Act alone were the basis of the request. It seems clear that they were enacted as desirable provisions in and of themselves, rather than as mere limitations upon the relatively small broadening of access achieved by the Privacy Act. If they are to be given such independent effect, they must be held applicable to all requests by file subjects and not just those citing the Privacy Act rather than the FOI Act.

Another substantial obstacle to the theory that the FOI Act and the Privacy Act afford alternate forms of procedures is the fact that neither Act requires the requester to identify the statutory provisions under which his request is made—and in fact many (if not most) current FOI requests do not contain such identification. Without specification, it would be impossible to determine which Act a particular request relied upon; and it is utterly implausible that Congress intended substantial effects to attach not merely to a Code citation, but to an executive or judicial surmise concerning which citation the requester would have used if he had used one.

CONCURRENT APPLICATION

Of course the foregoing objections could be overcome if the Privacy Act were to be considered not merely an alternative to the FOI Act but a supplement to it—that is, if both the FOI Act and the Privacy Act were to be considered applicable simultaneously to all requests by file subjects. Other provisions make it clear, however, that the two acts simply cannot be read entirely together.

For example, the Privacy Act, while prescribing time limits for the correction of records, prescribes no limits on the agency decision to grant or deny access to records. The FOI Act, on the other hand, sets rigid limits on the decision to grant or deny access.[1] Furthermore, the FOI Act provides that no exhaustion of administrative remedies is required if its time limits are not met; the Privacy Act, being silent on the subject, presumably requires exhaustion of administrative remedies.[2] The FOI Act requires notice, upon denial of access

[1] Compare 5 U.S.C. 552a(d)(1) with 5 U.S.C. 552(a)(6).
[2] Compare 5 U.S.C. 552(a)(6)(C) with 5 U.S.C. 552a(d)(1).

to records, that the individual may appeal that decision within the agency. The Privacy Act requires neither the internal appeal itself nor any notice of further rights after denial.[3] A party denied records under the FOI Act may obtain injunctive relief and costs and attorneys fees; no specific statute of limitations is provided. Similar relief is available under the Privacy Act but there is a two-year statute of limitations.[4]

Of course one might maintain that the two Acts were meant to be cumulative where not inconsistent, but where inconsistent the provisions of the later Act would prevail. Such an interpretation is cast into doubt by subsection (q) of the Privacy Act which specifically states that the FOI Act exemptions from disclosure cannot be used to deny an individual access to files about himself. There would be no need for such a provision if all inconsistencies between the two acts were to be resolved in favor of the later.[5]

Attempting to read the two acts as cumulative, at least in part, creates a scheme of enormous complexity. If they are to be read as complementary, except where inconsistent, it becomes necessary to determine when that inconsistency exists. For example, is the Privacy Act provision permitting special disclosure restrictions on medical records—limiting disclosure to a physician—consistent with the FOI provision on disclosure? Does 5 U.S.C. 552a(q) mean not only that the (b)(3) exemption of FOI cannot be used as a basis for denying records but also that the (b)(3) exemption for statutory restrictions on disclosure is unavailable?[6] Does the fact that the Privacy Act does not require an administrative appeal from a denial of access overrule the FOI requirements that such an appeal be provided and notice of its availability be given the requester? Reading the acts cumulatively, when would the administrative remedies be exhausted for purposes of seeking judicial review? If records are provided to the individual, what fees may be charged?[7]

Courts and administrators should not be cast upon this sea of uncertainty without a clear expression of congressional intent to that effect. That does not exist in the present case. To the contrary, in our view the Privacy Act bears every evidence of having been regarded as a self-contained unit, embodying all requirements that Congress intended from definitions to provisions of judicial review. It is, in our view, intended to be exclusively applicable to all cases in which an individual requests records from a system of records covered by the Privacy Act, after a date on which it comes into effect.

Sincerely,

MARY C. LAWTON,
Deputy Assistant Attorney General, Office of Legal Counsel.

EXHIBIT 2

U.S. SENATE,
Washington, D.C., August 26, 1975.

HON. EDWARD H. LEVI,
Attorney General, Department of Justice, Washington, D.C.

DEAR MR. ATTORNEY GENERAL: The Office of Management and Budget has recently circulated to all federal agencies a package of materials characterized as "helpful to your efforts to implement the Privacy Act of 1974." In this package, however, is a letter which clearly does *not* help agency efforts to implement the Privacy Act. This letter, written by Deputy Assistant Attorney General Mary

---

[3] Compare 5 U.S.C. 552(a)(6)(A)(i) with 5 U.S.C. 552a(d)(1).

[4] Compare 5 U.S.C. 552(a)(4) with 5 U.S.C. 552a(g)(5).

[5] Of course, the provision is also somewhat superfluous under the theory that the Privacy Act is exclusive, but it seems to be less so. If an intricate system were being established, hereby some provisions of the later Act would supersede those of the earlier, but others would not, one would expect more than a single expression of the practical operation of such supersedure. Assuming, however, that the entire Privacy Act was regarded as exclusive, subsection (q) can be seen as a somewhat superfluous but understandable affirmation of exclusivity in a particularly important area.

[6] Under the Veterans' Administration Statute, 38 U.S.C. 3301(1) records are not available to the veteran, if disclosure would be injurious to his physical or mental health. Under FOI, such records would be exempt from disclosure under 5 U.S.C. 552(b)(3)—records exempt by statute. What is their availability under Privacy Act?

[7] The FOI Act permits fees to be charged for the costs of both search and duplication, 5 U.S.C. 55(a)(4). Under the Privacy Act only duplication fees "excluding search" may be charged. 552a(f)(5).

Lawton, could prove pernicious and destructive if allowed to become the official Justice Department interpretation of the law.

Under the Freedom of Information Act the Department of Justice has a special leadership role in encouraging "agency compliance" with the FOIA. (5 U.S.C. § 552(d).) Miss Lawton's letter reflects a perversion of that role. I am thus appealing to you to review this matter and to issue guidance consistent with the congressional intent in both the Privacy and Freedom of Information laws.

The question raised is whether the Privacy Act of 1974 is the exclusive avenue available to a person requesting government records about himself, or whether the Freedom of Information Act may be applicable to such request. The Freedom of Information Act and its 1974 Amendments were enacted prior to final passage of the Privacy Act and therefore contain no reference to any possible interplay or conflict between the two laws. And it is true that the Privacy Act does not clearly address all aspects of the interface between them. Yet, regardless of specific inconsistencies between the provisions of the two laws, it would be manifestly unreasonable to conclude that Congress intended in the Privacy Act to carve out large implied exceptions to the requirements of the Freedom of Information Act. Generally supporting this observation are the following points:

1. The Freedom of Information Act exempts from mandatory disclosure matters "*specifically* exempted from disclosure by statute." (5 U.S.C. § 522(b)(3).) If the Privacy Act's exclusion of certain agencies or records does not "specifically" exempt them "from disclosure"—as opposed to merely exempting them from the application of certain Privacy Act provisions, then an exception to application of the FOIA's disclosure requirements cannot be sustained.

2. The Privacy Act was passed by Congress shortly after passage of the FOIA Amendments, which significantly strengthened disclosure requirements under the 1967 FOIA. (Further, the same House Committee—and Members—were responsible for managing both bills.) Implied repeal of statutory provisions are not generally favored: it would be especially unusual to conclude that Congress impliedly emasculated a public right in one bill that it had invigorated just a few weeks earlier.

3. Both House and Senate Reports on the Privacy Act refer with approval frequently to the FOIA. The final Privacy Act excepts from the disclosure limitations of section 552a(b) records required to be disclosed "under section 552 of this title" (the FOIA). It further provides in section 552a(q) that FOIA exemptions may not be invoked "to withhold from an individual any record which is otherwise accessible" to him under the Privacy Act. These clauses strongly imply that on the most basic questions—disclosure to a third party of government information about an individual, and disclosure to an individual of information about himself—Congress intended that FOIA and Privacy Act will be coordinated and applied consistently. (I should note that neither law requires its provisions to be invoked by reference. So it becomes even more important for the agencies themselves to initiate an integrated handling of requests under both.)

Miss Lawton's letter examines some of the procedural problems of applying the Privacy Act and FAOI alternatively or concurrently. She does not examine the more substantive problems of applying the Privacy Act exclusively:

1. Exclusive application of the Privacy Act would allow a blanket exemption from FOIA application for the entire CIA and FBI and for investigatory files in other agencies. Yet not only did Congress reject (both in 1966 and 1974) excluding the FBI and CIA from FOIA requirements, the FOIA Amendments expand public access, under carefully delineated guidelines, to investigatory and improperly classified documents. The Senate Judiciary Committee debated the question of applying the Act to the FBI and CIA. Much of the Senate floor debate was directed toward assessing the need for and implications of applying an amended seventh exemption (relating to investigatory files) to the FBI. And modification of the seventh exemption of the FOIA in Conference involved direct participation of the FBI with the staff of the managers. It is therefore unreasonable to conclude that, in view of the time and effort given moulding the FOIA to the unique problems of the FBI, Congress would have turned around and allowed that agency to be exempted completely from the Act without explicitly saying so.

2. One especially ludicrous result would ensue from treating the Privacy Act as exclusive as to covered records systems: a third party would be able to obtain more information from an investigatory file than the subject of that file himself.

For while the record could be exempt from access by the subject under the Privacy Act (sections 552a (j)-(k)), it would still be reachable under the FOIA. Moreover, if the requester obtained an affidavit from the subject, disclosure would not even constitute an "unwarranted invasion" of the subject's privacy (sections 552(b)(6)-(7)(c)). The Privacy Act's apparent exclusion (under this reading) could thus be simply circumvented by use of a straw-man.

I note that Miss Lawton concedes the possibility that the two Acts could be read "to be cumulative where not inconsistent" (page 4). She reasons, however, that if they were so read there would be no need for the Privacy Act to state that the FOIA exemptions "cannot be used to deny an individual access to files about himself." (Section 552a (q).) This is not only a superficial basis, on which to reject cumulative application of the two laws; it actually provides support for the opposite conclusion. The full clause reads:

"No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record *which is otherwise accessible to such individual under the provisions of this section.*" (Emphasis added.)

It appears clearly intended that access under the Privacy Act is to be complete, and not subject to FOIA exemptions, where the Privacy Act grants access. But where the Privacy Act does not grant access, the FOIA—and its exemptions—apply.

This, it seems to me, provides a coherent and rational approach for integrating the two laws substantively. Any other would do injury to the congressional purpose and national policy underlying each Act.

Once this substantive compatibility is accepted, there nonetheless remain complex and challenging procedural issues involving the interaction of the two laws. These may be resolved more readily if the objectives of both laws—broad access, agency responsiveness, and effective judicial review—are used to guide their resolution. I and the staff of the Subcommittee on Administrative Practice and Procedure stand ready to assist you and your staff in developing a coherent procedural framework, for agency handling of information requests, that is faithful to the requirements of both the Privacy Act and the Freedom of Information Act.

If, after the effective date of the Privacy Act, the FBI, CIA, IRS, or other agency refuses to provide information covered by the Freedom of Information Act on the grounds that the information is in record systems exempted from application of the Privacy Act, and that the Privacy Act is exclusive in that regard, I believe that refusal will ultimately be found to be arbitrary and capricious by the courts. These issues should not, in any event, have to await litigation for their resolution.

Since the Privacy Act becomes effective next month, and agencies are presently actively planning to implement that Act, your opinion on this issue of exclusivity is critically needed as soon as possible. I will look forward to your response.

Sincerely,

EDWARD M. KENNEDY.

EXHIBIT 3

LIBRARY OF CONGRESS, CONGRESSIONAL RESEARCH SERVICE,
Washington, D.C., September 8, 1975.

To: Senate Subcommittee on Administrative Practice & Procedure.
From: American Law Division.
Subject: Relationship of the Freedom of Information Act and the Privacy Act: Exclusivity of Remedies.

This is in response to your request for a critical analysis of the Justice Department's position regarding the relationship of the Freedom of Information Act (5 U.S.C. 552) and the recently enacted Privacy Act (5 U.S.C. 552a). It is the Department's position, as stated in a July 30, 1975 letter from Deputy Assistant Attorney General Mary Lawton to the Chief Counsel, Internal Revenue Service, that the Privacy Act after its effective date of September 27, 1975, is "the exclusive remedy for an individual who seeks records about himself contained in a system of records covered by the Privacy Act."

The Department's letter notes various provisions in the Privacy Act which limit access to an individual's files in arguing that the Privacy Act is not an alternative procedure to the Freedom of Information Act. Procedural variations between the two acts are pointed to as indicating "that the two acts simply cannot be read entirely together." Furthermore, according to the letter, "[a]ttempting to read the two acts as cumulative, at least in part, creates a scheme of enormous complexity." The letter concludes:

"Courts and administrators should not be cast upon this sea of uncertainty without a clear expression of congressional intent to that effect. That does not exist in the present case. To the contrary, in our view the Privacy Act bears every evidence of having been regarded as a self-contained unit, embodying all requirements that Congress intended, from definitions to provisions of judicial review. It is, in our view, intended to be exclusively applicable to all cases in which an individual requests records from a system of records covered by the Privacy Act, after the date on which it comes into effect."

The Privacy Act is a comprehensive law relating primarily to the safeguarding, management, compilation and dissemination of records maintained by the federal government on individuals and which are retrievable bp the name of the individual or some other identifying particular assigned to the individual. See, 5 U.S.C. 552a (a)(5). The principal aim is the protection of the privacy of the individual by controlling the disclosure of records pertaining to him and assuring that files are maintained accurately, with the individual's knowledge, and for a proper purpose. Access by an individual to records pertaining to him is accorded under subsection d(1) of the Act and means are provided by which amendments and corrections of the records can be made. 5 U.S.C. 552a(d)(2). Exemptions from the access and modification provisions, as well as other provisions of the Act, are permitted the agencies. 5 U.S.C. 552(a)(j) and (k).

The Freedom of Information Act (FOIA), 5 U.S.C. 552, is a disclosure law. It provides, inter alia, that upon request for records by any person, agencies shall make such records available unless they fall within the terms of nine exemptions to the Act. 5 U.S.C. 552(b). The exemptions relate to the substance of the records and permit the withholding of such matters as classified material, interagency memoranda, investigatory files, personnel and medical records, and records specifically exempt from disclosure by statute.

An individual can request records pertaining to him under the terms of both acts. The Privacy Act specifically grants him access under 5 U.S.C. 552a(d)(1). An individual is clearly "any person" under the FOIA and so long as the records are "reasonably described" (5 U.S.C. 552(a)(3)(A)) he can seek such records pertaining to himself under that act. The question is whether the Privacy Act is the exclusive means of obtaining access to records pertaining to the individual requester when such records are contained in a system of records as defined in the Privacy Act.

The Privacy Act contains four references to the Freedom of Information Act, none of which resolve the question of exclusivity of remedies. Section (b)(2) prohibits disclosure of any individually identifiable record to any person or agency, without prior request by or consent of the individual concerned, unless disclosure would be "required under section 552 of this title." 5 U.S.C. 552a (b)(2). Disclosures under (b)(2) are also exempt from the requirement that such records be "accurate, complete, timely, and relevant for agency purposes" before they are disseminated to any person other than an agency. 5 U.S.C. 552a (e)(6). Among the specific exemptions in the Act (which permit agency heads to exempt certain systems of records from various provisions of the Act) are systems of records "subject to the provisions of section 552(b)(1) of this title."[1] 5 U.S.C. 552a(k)(1). Finally, the Freedom of Information Act is mentioned in section (q) which prohibits an agency from relying on exemptions in the FOIA to withhold records from an individual otherwise accessible under the Privacy Act. 5 U.S.C. 552a(q).

The legislative history of the Privacy Act is similarly unilluminating on the question of the relationship of the remedies provided in both the Privacy Act and

[1] 15 U.S.C. 552(b)(1) is the first exemption of the Freedom of Information Act relating to matters that are "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive order."

the FOIA.[2] Congress was not oblivious to the requirements of the Freedom of Information Act, however, during consideration of the Privacy Act. In fact, the President's veto of amendments to the FOIA designed to facilitate disclosure of records was overridden on the same day the Privacy Act was approved. The veto override vote in the House came within minutes of the debate and passage of the House version of the Privacy Act.

A version of the Privacy Act which passed the Senate on November 22, 1974 contained a provision that "[n]othing in this Act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder." See, 120 Cong. Rec. S 19900 (daily ed. Nov. 22, 1974). This provision was omitted from the final version without explanation. Sections (b)(2) and (q) were instead added to the bill which became the Privacy Act. The Analysis of House and Senate Compromise Amendments to the Federal Privacy Act submitted in lieu of a conference report explains, somewhat ambiguously:

"The Senate bill reflected the position of an earlier draft of the House measure in Section 205(b) where it provided that nothing in the act shall be construed to permit the withholding of any personal information which is otherwise required to be disclosed by law or any regulation thereunder. This section was intended as specific recognition of the need to permit disclosure under the Freedom of Information Act.

"The compromise amendment would add an additional condition of disclosure to the House bill which prohibits disclosure without written request of an individual unless disclosure of the record would be pursuant to Section 552 of the Freedom of Information Act. This compromise is designed to preserve the status quo as interpreted by the courts regarding the disclosure of personal information under that section.

"A related amendment taken from the Senate bill would prohibit any agency from relying upon any exemption contained in Section 552 to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section." 120 Cong. Rec. S. 21817 (daily ed., Dec. 17, 1974).

Thus, the intention of the compromise amendments described above was to "preserve the status quo as interpreted by the courts regarding the disclosure of personal information under [the FOIA]." Since the status quo included the possibility of individual access to his own file under the FOIA, it can hardly be persuasively argued that the omission of the language of the Senate-passed bill in the final version and its replacement with the compromise amendments "suggests that Congress ultimately decided that the Privacy Act exemptions should govern exclusively . . ."[3] While it is true that the effect of the compromise amendments differs from that of the Senate-passed bill, it is the intent of the Congress as an interpretative device which is important. Silence on the omission of a provision and an intent to preserve the statute quo vis-a-vis the FOIA respecting other provisions can not be read to mean that Congress intended to replace the FOIA with the mechanisms of the Privacy Act regarding individual access to his own file.

Speculation over Congressional intent is risky, particularly in the case of a complex bill passed rather hurriedly at the end of a legislative session. Those who argue that the Privacy Act preempts the FOIA in cases of individuals seeking their own records contained in a system of records, however, must overcome some basic tenets of statutory interpretation.

The Justice Department argument is that the Privacy Act implicitly worked an amendment or repeal of the FOIA in that class of cases involving an individual seeking disclosure of a record pertaining to him contained in a system of records as defined in the Act. However, repeals or amendments by implication are not favored. *Regional Rail Reorganization Act Cases*, 419 U.S. 102, 133 (1974); *Morton* v. *Mancari*, 417 U.S. 535, 550 (1974); *Posadas* v. *National City*

---

[2] The Senate reported a privacy bill, S. 3418, on September 26, 1974. S. Rept. No. 93-1183. The House version, H.R. 16373, was reported on October 2, 1974. H. Rept. No. 93-1416. The bills were debated by both houses on November 20 and 21, 1974 and different versions were passed by the House and Senate on November 21. See, 120 Cong. Rec. H 10884–10902, S 19823, 19826–19862, H 10950–10972 (daily ed. Nov. 20, 21, 1974). A conference was not held on the differing bills, but a staff compromise was presented and debated on December 17 and 18, 1974. See, 120 Cong. Rec. S 21808–21823, H 12242–1224, S 21995–21996 (daily ed. Dec. 17, 18, 1974). The Privacy Act became law on December 31, 1974.

[3] Lawson letter, p. 2.

Bank, 296 U.S. 497, 503 (1936). "In the absence of some affirmative showing of an intention to repeal, the only permissible justification for a repeal by implication is when the earlier and later statutes are irreconcilable." *Morton* v. *Mancari*, 417 U.S. 535, 550 (1974). The Supreme Court, in the *Regional Rail Reorganization Act Cases*, agreed with the District Courts' formulation of the rule:

"A new statute will not be read as wholly or even partially amending a prior one unless there exists a "positive repugnancy" between the provisions of the new and those of the old that cannot be reconciled. . . . Before holding that the result of the earlier consideration has been repealed or qualified, it is reasonable for a court to insist on the legislature's using language showing that it has made a considered determination to that end." 419 U.S. 102, 134 quoting 384 F. Supp. 895, 946 (Sp. Ct. 1974).

The question in the rail reorganization cases cited above was whether the Rail Act, with its own remedy and scheme of compensation, preempted the general Tucker Act remedy for unconstitutional takings of property. See 419 U.S. 102, 126. The Supreme Court held that it did not.[4] As a general rule, remedial statutes are given a harmonious construction if possible and "the enactment of a new statutory remedy does not operate to repeal other statutory remedies, but the new remedy is construed as cumulative and to coexist with the existing methods of enforcement." Sutherland, *Statutory Construction* § 23.27 (4th ed. 1974); see, *Jones* v. *Mayer Co.*, 392 U.S. 409, 416 (1968); *Sullivan* v. *Little Hunting Park*, 396 U.S. 229, 237 (1969).

The Department of Justice points to several differences in the access provisions of the Privacy Act as opposed to the FOIA as creating a "sea of uncertainty" and evincing an intent on the part of Congress to replace the FOIA remedy with the Privacy Act remedy, "a self-contained unit, embodying all requirements that Congress intended, from definitions to provisions of judicial review." As noted above, it is difficult to argue that Congress intended such a drastic remedial modification without saying a word about it and on the same day it overwhelmingly overrode a Presidential veto of a strengthened version of the very act it is now argued was modified. Furthermore, an examination of the "inconsistencies" discussed in the Department's letter does not demonstrate the degree of irreconcilability and "repugnancy" necessary on which to base a conclusion of qualification or repeal by implication. See, Sutherland, supra § 23.10; *Posadas* v. *National City Bank*, 296 U.S. 497, 504 (1936); *Regional Rail Reorganization Act Cases*, 419 U.S. 102, 134.

The Department's letter mentions three provisions of the Privacy Act which serve to *limit* access to information and argues that such limitations, contained as they are in the newer statute, preclude alternative use of the older FOIA. However, exemptions or limitations contained in later remedial statutes do not necessarily evidence an intent to occupy the field to the exclusion of earlier remedial statutes on the same subject. See, *Jones* v. *Mayer Co.*, 392 U.S. 409, 416 (1968);[5] *Sullivan* v. *Little Hunting Park*, 396 U.S. 229 (1969).[6] Furthermore,

---

[4] In analyzing egislative history which is relatively more illuminating than that available on the similar question in the context of the Privacy Act and the FOIA, the Court concluded:

"In sum, we cannot find that the legislative history supports the arguments that the Rail Act should be construed to withdraw the Tucker Act remedy. The most than can be said is that the Rail Act is ambiguous on the question. In that circumstance, applicable canons of statutory construction require us to conclude that the Rail Act is not to be read to withdraw the remedy under the Tucker Act." 419 U.S. 102: 133.

[5] Title VIII of the Civil Rights Act of 1968 did not affect 42 U.S.C. § 1982, despite the fact that the former contains exemptions and time limits not contained in the latter. The Court stated:

"At oral argument, the Attorney General expressed the view that, if Congress should enact the pending bill, § 1982 would not be affected in any way but "would stand independently." That is, of course, correct. The Civil Rights Act of 1968 does not mention 42 U.S.C. § 1982, and we cannot assume that Congress intended to effect any change, either substantive or procedural, in the prior statute." 392 U.S. 409, 416 n. 20.

See also, *Fred* v. *Kokinokos*, 347 F. Supp. 942. (E.D. N.Y. 1972).

[6] Civil Rights Act of 1964 did not supersede 42 U.S.C. § 1982. The court in *Tsoy* v. *Shell Oil Company*, 378 F. Supp. 1042, 1047 (E.D. Mich. 1974) elaborated:

"The distinction between a Title VII claim and a claim bottomed on the Civil Rights Act of 1866 is significant. A claimant under the latter is not burdened with the procedural prerequisites of Title VII. Although the kinds of discrimination covered by the two statutes overlap to some extent, the courts have nevertheless refused to hold that the older statute was preempted by Title VIII. The remedies they create are indepndent and unaffected by the other's existence. . . . Thus, when discrimination of the type covered by both statutes is involved, relief may be available under § 1981 et seq. which is not available under Title VII because of a failure to exhaust administrative remedies."

See also, *Penn* v. *Schlesinger*, 497 F. 2d 970 (5th Cir. 1974).

administrative interpretations of two of the three provisions result in no incompatibility with the FOIA.

For instance, the Department's letter notes that agencies may impose identity verification requirements on individuals seeking access to their records under the Privacy Act. 5 U.S.C. 552a(f)(2). There is no similar requirement under FOIA. However, OMB has recommended regarding (f)(2) verification that the "requirements pertaining to verification of identity contained in subsection (f)(1) [notification of an individual that a record pertaining to him exists], above, should also be noted." OMB Guidelines 28967. Subsection (f)(1) verification procedures "may only be imposed when the fact of the existence of a record would not be required to be disclosed under the Freedom of Information Act (5 U.S.C. 552)." OMB Guidelines 28967; see OMB Guidelines 28964.

Thus, an effort is made to mesh the two acts. Furthermore, as a practical matter, verification procedures are likely to be employed in FOIA requests for such individually identifiable records. The disclosure of a record to someone other than the subject of that record may "constitute a clearly unwarranted invasion of personal privacy" (5 U.S.C. 552(b)(6), while disclosure to the individual himself may not. Thus, some verification procedure is necessary to determine the applicability of the FOIA exemption. See also, 5 U.S.C. 552(b)(7)(C).[7]

The Department's letter also points to the supposed conflict between the FOIA and subsection (f)(3) of the Privacy Act which, in its view, "permits an agency to restrict certain disclosures to the requesting subject's physician rather than making them to the subject himself."[8] OMB does not seem to take such an either/or position nor do the terms of the Act reflect such a position. Subsection (f)(3) does permit special procedures "if deemed necessary", but these special procedures are for "the disclosure *to an individual* of medical records." (Emphasis supplied). The OMB Guidelines similarly provide:

"As written, the Act provides that individuals have an unqualified right of access to records pertaining to them (with certain exceptions specified in subsections (j) and (k), below, but that the *process* by which individuals are granted access to medical records may, at the discretion of the agency, be modified to prevent harm to the individual." OMB Guidelines 28967 (Emphasis added).

Finally, the Department views subsection (d)(5) as a limitation making alternative application of the Privacy Act and the FOIA impossible. Subsection (d)(5) provides that "nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding." 5 U.S.C. 552a(d)(5). The Department concludes (apparently with regard to this subsection and the others discussed above) that "it is entirely implausible that such substantial protections as these were intended only to apply to the incremental access which the Privacy Act provides beyond that of the FOI Act—so that they could be entirely avoided if the FOI Act alone were the basis of the request."[9]

Initially, it might be said that entirely avoiding the restrictions of (d)(5) by means of the FOIA may be difficult in many, if not most, situations as exemption 7 of the FOIA may well apply to such records. Secondly, the OMB Guidelines interpret subsection (d)(5) within the framework of the FOIA:

"This provision is not intended to preclude access by an individual to records which are available to that individual under other procedures (e.g. pretrial discovery). It is intended to preclude establishing by this Act a basis for access to material being prepared for use in litigation other than that established under other processes such as the Freedom of Information Act or the rules of civil procedure." OMB Guideline 28960.

---

[7] In discussing this portion of exemption 7 of the FOIA in the Conference Report on the 1974 amendments, it was stated that the conferees "wish to make clear that disclosure of information about a person to that person does not constitute an invasion of his privacy." Some identity verification procedures would seem to be necessary in order to determine the applicability of this exemption. The Attorney General also states that "when information otherwise exempt under clause (c) is sought by a requester claiming to be the subject of the information, the agency may require appropriate verification of identity." Attorney General's Memorandum on the 1974 Amendments to the Freedom of Information Act 10 (1975).

[8] Lawton letter, page 3.

[9] Id.

Thus, subsection (d)(5) would seem to leave the FOIA unimpaired.

Other procedural variations between the two Acts are noted by the Department in arguing that the Privacy Act and the FOIA are incapable of concurrent application. The Privacy Act prescribes no time limits on the agency decision to grant or deny access to records unlike the FOIA which sets limits. Neither does it require an administrative appeal of the denial of access to records. A two-year statute of limitations is applicable to civil relief under the Privacy Act. The FOIA has no specific statute of limitations provision.

Regarding the time limits, OMB has recommended that agencies reply to a request for access within 10 days, the same as under FOIA, OMB Guidelines 28957. Furthermore, the fact that the Privacy Act dispenses with the necessity of administrative appeal and has no set exhaustion of remedies schedule as in the FOIA does not preclude harmonizing the two Acts. As the Department's letter recognizes, "[t]here would be no difficulty in harmonizing application of the two Acts to the same request if the effect of the Privacy Act were merely to expand access which the FOI Act already provides. Then one might reasonably assert that a requester was free to proceed under the older legislation—but could obtain still more by proceeding under the newer." [10]

An alternative interpretation—and a means to harmonize the two Acts—would be to impose the FOIA procedural requirements (time limits, appeal rights) on requests for records in a system of records. Congressional silence could mean that it intended such limits to apply. Access is not a new remedy provided by the Privacy Act and the machinery of the FOIA, in terms of administrative handling of requests, is already in existence. On the other hand, Congress did feel it necessary to prescribe time limits in the newer legislation when it provided for a new remedy, namely, the correction of individual records. 5 U.S.C. 552a(d)(2). A request for one's record contained in a system of records comes within the terms of the FOIA [11] and nothing in the Privacy Act explicitly prohibits application of the general terms of the FOIA.

It would seem that the procedural variations between the Privacy Act and the FOIA do not pose insurmountable barriers to a harmonizing interpretation and application of the two acts. They certainly do not point to a complete supersedure by the Privacy Act of the FOIA with respect to individuals' requests for their own records contained in a system of records. An examination of the substantive provisions of the Act—particularly the operation of the Privacy Act's exemptions in relation to FOIA requests for similar records—demonstrates the absurd consequences of viewing the Privacy Act as the exclusive means of gaining access to one's own records.

Sections (j) and (k) of the Privacy Act permit agencies to exempt certain systems of records from various provisions of the Act, including (d)(1), the access provision. The general exemptions in section (j) allow institutional exemptions for files maintained by the CIA and law enforcement agencies. The section (k) specific exemptions relate to the substance of the records and include records subject to (b)(1) of the FOIA (classified national security matters), investigatory records, records maintained in connection with protection of the President, purely statistical records, and records relating to qualification, testing, promotion, appointment for various forms of federal service.

The exemptions do not apply to section (b) of the Privacy Act, which outlines conditions of disclosure to third parties of an individual's records. Section (b) prohibits such disclosure without prior request or consent of the individual unless disclosure would be "required under section 552 of this title [FOIA]." 5 U.S.C. 552a(b)(2). Thus, a third party could gain access to an individual's record contained in a system of records if none of the exemptions of the FOIA

---

[10] Lawton letter, page 2.

[11] 5 U.S.C. 552(a)(3) provides:

"Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, upon any request for records which (A) reasonably describes such records and (B) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person."

The FOIA speaks in terms of "any request" for records, not just requests for records pursuant to this section.

applied to the records.[12] The anomaly of greater third-party access to an individual's file than the individual himself could thus result if the Privacy Act exemptions are broader than the FOIA exemptions and the Privacy Act is deemed the exclusive vehicle for individual access to his own records.

For example, assuming the Justice Department's position that the Privacy Act is exclusive, records maintained by the CIA, regardless of their content, may be exempt from the access provision of the Privacy Act. 5 U.S.C. 552a(j)(1). However, if the substance of the records does not entitle them to come under any of the nine exemptions of the FOIA, a third party would have access to the records pursuant to the FOIA and section (b)(2) of the Privacy Act.[13]

The breadth of some of the specific exemptions might also contribute to the anomaly described above. For example, records "maintained and used solely as statistical records" could be denied the individual (5 U.S.C. 55a(k)(3)), but be available to third parties under the FOIA, assuming no FOIA exemption applied. Similarly with records "maintained in connection with providing protective services to the President of the United States or other individuals", a broad exemption not keyed to the specific content of a record. 5 U.S.C. 552a(k)(4). Exemption 2 of the specific Privacy Act exemptions covers "investigatory material compiled for law enforcement purposes", a much broader exemption than the comparable law enforcement exemption of the FOIA.[14] Since exemption 7 is a frequently invoked exemption in FOIA cases, it is likely that the third party versus individual access question may arise in this context.

The difference between third-party and individual access as a result of the Justice Department's interpretation of the exclusivity of remedies also points to the ease which the limitations resultant from exclusivity may be circumvented. If an individual is denied access to records which would be available under the FOIA, all he need do, assuming he is precluded from pursuing an FOIA remedy himself, is to ask a friend to request them for him. The records would have to be disclosed pursuant to section (b) of the Privacy Act, either because the individual has submitted a written request that they be disclosed to the third party or because they are required to be disclosed under section 552 (FOIA). 5 U.S.C. 552a(b)(2).

The absurdity of the above results—greater third-party access and the promotion of circumvention—probably argues more persuasively against the exclusivity argument of the Justice Department than an effort to reconcile the minutiae of differing procedural requirements. Statutes will not be interpreted to reach absurd results.[15] Since there is no provision prohibiting recourse to the FOIA remedy nor legislative history indicating that the FOIA remedy has been superseded, the Privacy Act remedy should not be construed in a manner which will result in the anomalies described above.

---

[12] One of the exemptions, (b)(6), of the FOIA permits the withholding of "personnel and medical files and similar files the dislosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. 552(b)(6).

The compromise final version of the Privacy Act rejected a provision of the House bill which would have made disclosure of all individually identifiable information in government files a "clearly unwarranted invasion of personal privacy" and thus exempt from disclosure under FOIA. See, 120 Cong. Rec. S21817 (daily ed., Dec. 17, 1974). Thus, it is possible that some individually identifiable records would not be exempt under the standards of 5 U.S.C. 552(b)(6) and thus required to be disclosed (assuming other FOIA exemptions were not applicable) to third parties under (b)(2) of the Privacy Act.

In addition, it would not seem that the Privacy Act is a statute under the terms of exemption 3 of the FOIA which permits withholding of matters "specifically exempted from disclosure by statute." 5 U.S.C. 552(b)(3). The exemptions in the Privacy Act are permissive and an agency is not *required* to withhold records within the purview of the exemptions. See OMB Guidelines 28971. Thus, any exemptions from disclosure under the Privacy Act is "the creature of the administrator and does not fall within the meaning of the words 'specifically exempted . . . by statute.'" *People of State of California* v. *Weinberger*, 505 F. 2d 767 (9th Cir. 1974); see, *FAA Administrator* v. *Robertson*, 45 L. Ed. 2d 164 (1975).

[13] It is likely that agencies will not exempt records from the terms of the Privacy Act if they would be available under FOIA, according to an OMB official connected with the drafting of the guidelines.

[14] Access to such investigatory records is expanded if "any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material . . ." 5 U.S.C. 552a(k)(2).

No such showing of injury is required for access under the FOIA.

[15] See, 73 Am. Jur. 2d *Statutes*, § 265.

CONCLUSION

There is nothing in the terms of the Privacy Act or its legislative history which indicates that the Privacy Act is the exclusive means by which an individual can gain access to his own records contained in a system of records. Many of the so-called "inconsistencies" listed in the Justice Department's letter have been reconciled with the FOIA in the OMB guidelines issued pursuant to the Privacy Act. Furthermore, they do not seem to constitute the clear repugnancies which are necessary before a court will hold that one statute has implicitly repealed or superseded another.

The primary purpose of the Privacy Act is the protection of individual privacy by controlling the collection, management, and dissemination of individually identifiable records. Access to such records by the individual is one method by which control is achieved and is a necessary adjunct to the accurate maintenance of records. It flies in the face of the whole legislative effort in this area to construe the Privacy Act as a backhanded method to limit individual access to records while at the same time preserving potentially greater access rights to third parties.

RICHARD EHLKE,
Legislative Attorney.

EXHIBIT 4

OFFICE OF THE DEPUTY ATTORNEY GENERAL,
Washington, D.C., October 1, 1975.

HON. EDWARD M. KENNEDY,
U.S. Senate, Washington, D.C.

DEAR SENATOR KENNEDY: I recently received a copy of your letter to Attorney General Levi expressing your concern about Deputy Assistant Attorney General Lawton's letter and the Justice Department's interpretation of the Privacy Act as ostensibly expressed in her letter.

Some weeks before I saw your letter, I and others here had concerns substantially similar to yours. Hence we discussed and drafted an additional provision to be added to our Privacy Act regulations. We think this provision, a copy of which is enclosed, serves to meet what you suggest.

That is not to say, however, that this provision will resolve all of the difficult procedural issues posed by the various sections of the two Acts. For that reason, I welcome your suggestion for a cooperative effort and have so notified my principal advisors. The Chief Counsel of your Subcommittee will be contacted shortly in this regard.

Sincerely,

HAROLD R. TYLER, Jr.,
Deputy Attorney General.

SECTION 16.57. RELATIONSHIP OF PRIVACY ACT AND THE FREEDOM OF INFORMATION ACT

(a) Issuance of this section and actions considered or taken pursuant hereto are not to be deemed a waiver of the Government's position that the materials in question are subject to all of the exemptions contained in the Privacy Act. By providing for exemptions in the Act, Congress conferred upon each agency the option, at the discretion of the agency, to grant or deny access to exempt materials unless prohibited from doing so by any other provision of law. Releases of records under this section, beyond those mandated by the Privacy Act, are at the sole discretion of the Deputy Attorney General and of those persons to whom authority hereunder may be delegated. Authority to effect such discretionary releases of records and to deny requests for those records as an initial matter is hereby delegated to the appropriate system managers as per the Notices of Systems of Records published in 40 *Federal Register* 167, pages 38703–38801 (August 27, 1975).

(b) Any request by an individual for information pertaining to himself shall be processed solely pursuant to Subpart D of these regulations. To the extent that the individual seeks access to records from systems of records which have been exempted from the Provisions of the Privacy Act, the individual shall re-

ceive, in addition to access to those records he is entitled to receive under the Privacy Act and as a matter of discretion as set forth in subsection (a), access to all records within the scope of his request to which he would have been entitled under the Freedom of Information Act, 5 U.S.C. 552, but for the enactment of the Privacy Act and the exemption of the pertinent systems of records pursuant thereto. Only those fees set forth in section 16.46 of this Title may be charged a requester as to any records to which access is granted pursuant to the provisions of the subsection.

(c) When an individual requests access to records pertaining to criminal, national security or civil investigative activities of the Federal Bureau of Investigation which are contained in systems of records exempted under provisions of the Privacy Act, such requests shall be processed as follows:

(1) Where the investigative activities involved here have been reported to F.B.I. Headquarters, records maintained in the F.B.I.'s Central filed will be processed; and

(2) Where the investigative activities involved have not been reported to F.B.I. Headquarters, records maintained in files of the Field Office identified by the requester will be processed.

CHAPTER III

Explanatory Articles and Criticism of the Act

[From Federal Bar Journal (Vol. 34; 279), Spring 1975]

The Privacy Act of 1974—Exceptions and Exemptions

(By James H. Davidson)[1]

The Privacy Act of 1974 reflects a Congressional effort to establish a "Code of Fair Information Practices" which applies to each agency of the Federal Government. That code mandates that the public as well as individual record subjects will play an important role in future personal information practices.

Without exception, agencies must make public a description of each system of records which they maintain about individuals. Beyond this requirement, however, there are few provisions of the Act which are not subject to some exceptions.

There are rules for the transfer of personal information between or outside Federal agencies, including a requirement that material transferred to someone other than a Federal agency must be checked for accuracy, relevance, timeliness and completeness. That does not apply, however, in the case of a transfer under the Freedom of Information Act.[2]

Other provisions of the Act grant individuals the right of access and challenge to information about them in Federal files. This too is limited by more detailed exemptions for certain kinds of information such as that pertaining to national security, law enforcement and information obtained from "confidential sources."

It is important to understand the operation of these exceptions and exemptions and the Congressional intent behind them in order to deal with the Act as a whole.

The forces seeking greater disclosure of government operations and information often are found in opposition to forces seeking protection of individual privacy. Some of the leading cases interpreting the Freedom of Information Act deal with the kinds of information about individual citizens which can be released without invading their privacy.

In hearings on the Privacy Act, former HEW Secretary Elliot L. Richardson, who commissioned the study sponsored by that Department entitled "Records, Computers and the Rights of Citizens," outlined the elements of this conflict:

"Public policy about the management of information must embrace three policy objectives," freedom of expression; personal privacy; and the public's right to know. In a free society these three objectives are always in contention, and the challenge to public policy is to strike a proper balance among them. No public policy on the management of recorded information about people can be formulated that will accommodate all three of these objectives if the right of personal privacy is understood as the right to be let alone. Freedom of expression and the public's right to know require trafficking in information in ways that impact on people. The issues that arise in achieving these objectives relate to how people will be affected—not whether they will be affected. Records about people are made to mediate and reflect actions affecting them."[3]

By an accident of scheduling, the override of the President's veto of the 1974 Amendments to the Freedom of Information Act and the Privacy Act were debated on the same days in the House and Senate. In many instances, Senators, Congressmen, and the staff involved in one, played important roles in the adoption of the other. It was not without considerable deliberation, therefore, that the mechanism in section b(2) of the Act was chosen to allow present case law to control in the balance between requests for public disclosure of information held by the government and the need to protect the privacy of individual citizens.

---

[1] Counsel, Senate Government Operations Subcommittee on Intergovernmental Relations.
[2] Public Law 93–579, Section e(6).
[3] Hearings, Ad Hoc Subcommittee on Privacy and Information Systems of the Committee on Government Operations and the Subcommittee on Constitutional Rights, Committee on the Judiciary, United States Senate, 93d Cong., 2d sess. Part I (1974).

Section b(2) states that: "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior consent of the individual to whom the record pertains unless disclosure of the record would be required under section 552 of this title." [4]

In other words, if information about an individual would be released under an FOI Act request, it could be released under b(2) of the Privacy Act. The standard for release under the FOI Act is in Section b(6) which permits the withholding of informtaion the release of which would constitute a "clearly unwarranted invasion of personal privacy." [5]

Under that test the courts have granted to law professors the lists of labor union members for a study of union voting.[6] In another case, a court of appeals ordered a U.S. District Judge to grant a law student cacess to those portions of Air Force Academy honor code proceedings which the District Judge reviewed and determined would not identify the subjects.[7] In yet another, a company producing wine-making kits was denied the right to see IRS lists of persons allowed to make wine without paying a tax.[8]

Finally, a plaintiff pursuing a class action against an airline sought in a separate FOI suit the names and addresses from customs declarations of all passengers of that airline who had flown for several months to one area of the world. In denying that request last July, the District Court for the District of Columbia seemed to equate a "substantial" invasion of privacy with the statutory standard of a "clearly unwarranted invasion" and also asserted that the fact the information was possible to obtain in other forms would support the withholding in that case.[9]

Only four months earlier a U.S. District Court in Florida ordered disclosure of similar forms, holding that to fall within the exemption they "must have the same characteristics of confidentiality that ordinarily attach to information in medical or personnel files; that is to such extent as they contain "intimate details of a highly personal nature; they are within the full umbrella of the exception." [10]

While the case law has not been consistent in all instances, it suggests that decisions on what information to release and what to withhold should be determined on a case-by-case basis. In adopting the Privacy Act, Congress set out broad guidelines for the handling of information about individuals by Federal agencies. Legislation prohibiting the disclosure of specific types of information should be approached on a subject-by-subject basis after more experience is gained in the implementation of this new law.

Until more precise limitations can be fashioned for certain categories of information, Congress endorsed the protection accorded personal information by the courts under section b(6) of the Freedom of Information Act.

That section is unique among the categories of exempted material under the FOI Act. It is the only exemption for which the Congress specifically called for a balancing of interests—that of public disclosure on the one hand, and the privacy of the individual on the other.

The Senate report on the 1966 FOI Act states: "The phrase 'clearly unwarranted invasion of personal privacy' enunciates a policy that will involve a balancing of interests between the protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information. The application of this policy should lend itself particularly to those Governmental agencies where persons are required to submit vast amounts of personal data usually for limited purposes. . . ." [11]

While the legislative history speaks of a balance between the protection of an individual's private affairs and the preservation of the public right to governmental information, the cases have varied in their definition of the public interest.

In *Getman*, the Court of Appeals for the District of Columbia said that the requirement to balance interests under b(6) was in unavoidable conflict with

---

[4] Public Law 93–579, Section b(2).
[5] U.S.C. 552 (b) (6).
[6] *Getman* v. *National Labor Relations Board*, 450 F.2d 670 (D.C. Cir. 1971).
[7] *Rose* v. *Department of the Air Force*, 495 F.2d 261 (2d Cir. 1974).
[8] *Wine Hobby U.S.A., Inc.* v. *United States Internal Revenue Service*, 502 F.2d 133 (3d Cir. 1974).
[9] *Ditlow* v. *Shultz*, 379 F. Supp. 326 (D.D.C. 1974).
[10] *Levine* v. *United States*, 42 LW 2526 (S.D. Fla. 1974).
[11] Senate Report No. 248, 90th Cong., 1st sess. 9 (1967).

the purpose of the 1967 Freedom of Information Act to limit agency discretion not to disclose by abandoning the former ground rule that a person requesting information show he was "properly and directly concerned." [12]

The Court made it plain that its ruling for the law professors should not be understood automatically to compel the Board in the future to give out *Excelsior* lists to all other applicants, and for other elections. "A request by less well qualified applicants, or applicants with a less carefully designed or more disruptive study would require a new balancing and might be found to involve a 'clearly unwarranted invasion of personal privacy' which would justify nondisclosure." [13]

Similar reasoning was adopted by the Third Circuit last year when it denied a request by Wine Hobby USA, Inc. for the names and addresses of taxpayers granted exemptions to produce home-made wine, asserting:

"Wine Hobby advanced no direct or indirect public interest purpose in disclosure of these lists and indeed, we can conceive of none. The disclosure of names of potential customers for commercial business is wholly unrelated to the purposes behind the Freedom of Information Act and was never contemplated by Congress in enacting the act." [14]

In *Wine Hobby*, the Third Circuit also specifically chose to ignore the reasoning of the Fourth Circuit in a 1973 decision, *Robles* v. *EPA*, granting access to the names and addresses of homeowners whose property had been built on radioactive landfill. In *Robles* the Court said that since the 1967 Act, the public interest and not the interest of the requestor was controlling.[15]

I believe that *Getman* and *Wine Hobby* do not carry forward the intent expressed in the 1967 FOI Act and refirmed by the 1974 Amendments, that it is the public interest and not the interest of the requestor which should be decisive in granting a request. Both of these cases could have been decided within that principle and still have protected the names of the individual citizens involved.

Robles is important for another element of the decision—the decision to release the names and addresses rested in part on the fact that these names also were available by arrangement with the Colorado Department of Health, although the degree of availability is not clear from the decision.

As with any law of this breadth, there must be a procedure for the protection of information which is sensitive to the national security, to the operation of law enforcement agencies or for other limited reasons.

Section (j) permits the head of a federal agency to use informal rulemaking procedures under the Administrative Procedures Act to exempt those systems of records which are maintained by the CIA or for criminal law enforcement. In so doing, the agency head must include the reasons for the exemption from any provision of the Act.

The exemptions permitted under section (j) and those under section (k) are framed in general terms. The categories could not be drafted with the kind of precision that would assure their most limited applications. By requiring open rule making with the receipt of comments and an agency statement explaining the exception for certain categories of records, the Congress was trying to avoid creation of a loophole which would permit entire agencies to avoid compliance with the Act.

There still is no exemption permitted by agencies from sections of the Act which prescribe the conditions for disclosure or exchange of information, which require accounting for such disclosures and the establishment of administrative rules and safeguards for personal information, which restrict the keeping of records on first amendment activities or which require an annual public notice listing all systems of records maintained by the agency, among others.

This is not an invitation to an agency to announce a *carte blanche* exemption for other portions of every record in its files. Rather they are urged to continue present policies of disclosure of records to their subjects and to expand those policies where possible.

These exemptions follow closely the House version of the bill. The Senate bill would have permitted exemptions only for certain law enforcement investigative and intelligence files. The broader exemption for systems of records

---

[12] Getman at 677, n.24.
[13] Id.
[14] Wine Hobby USA, Inc. v. IRS, at 137.
[15] Robles v. Environmental Protection Agency, 484 F.2d 843 (4th Cir. 1973).

maintained by any agency or component whose principal function pertains to criminal law enforcement was accepted in deference to still active efforts in both the House and Senate to pass criminal justice information legislation.[16]

The CIA exemption was broadened from a protection in the Senate bill of national defense and foreign policy material only after an agreement was reached to pursue further the appropriate type of exemption for the protection of intelligence sources and methods.

Agency heads may apply for more narrow exemptions from the act under section (k) where a system of records falls within one of the following seven categories:

Material which may be withheld for national defense and foreign policy reasons under the first exemption of the Freedom of Information Act. Under the new amendments to that act such documents must be both properly classified and "classifiable";

Material compiled for law enforcement. This is to include that material used by various agencies for civil law enforcement which would not be covered by the (j) exemption;

Records maintained by the Secret Service for the protection of the President;

Records maintained for statistical or reporting purposes and not used in making a determination about an identifiable individual;

Investigatory material compiled for determining suitability for federal employment or military service;

Testing or examination material the revelation of which would compromise the federal testing procedures and give some competitors an unfair advantage; and

Material used to evaluate potential for promotion in the armed services.

In addition to the requirements which agencies that exercise the (j) exemption must meet with regard to those excepted systems of records, records exempted under (k) must also comply with the following requirements:

Inform prior recipients of corrected or disputed records;

To collect information to the greatest extent practicable from the individual to whom it pertains;

To inform individuals asked to supply information whether it is mandatory they comply with the request and the purpose for which the information will be used;

To maintain records with such accuracy, completeness, timeliness, and relevance as is reasonable for the agency's purposes;

To notify the subjects of records which have been disclosed pursuant to compulsory process once that process has become a matter of public record; and

The civil remedies and sanctions for violations of the act.

By making a distinction between the general (j) and specific (k) exemptions, the Congress indicated its view that the latter would involve a much smaller percentage of an agency's total system of records than would the CIA and criminal law enforcement exemptions.

Particular mention should be accorded three categories of the (k) exemption—those for civil law enforcement, for suitability investigations and for armed services promotion evaluations.

Agencies may promulgate rules to withhold information falling within these categories only to the extent that the disclosure of material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence. Prior to September 27, 1975, the effective date of this Act, information received under an implied promise of confidentiality will support the withholding.

Access to civil law enforcement investigatory material would be permitted under these conditions only when an individual has been denied a right, benefit, or privilege to which he otherwise would be eligible because of agency use of the material.

The House language governing confidential source protection was agreed to only after considerable debate between the chairmen and ranking minority members of the Senate Government Operations Committee and the House Subcommittee on Foreign Operations and Government Information.

---

[16] See S. 1427, S. 1428 and H.R. 62, introduced in the 4th Congress.

It was included in this Act to assure individual access to files which in part have been accorded great secrecy but which bear the potential for great harm to the subject. It was the intent of the Congress to encourage the collection of only that investigatory information essential to a proper evaluation of a person's employability or advancement. If it is determined to be necessary to obtain information from another party, an express promise of confidentiality should be given only when there is no other way to obtain the third-party view.

Finally, an individual should be granted access to all portions of such investigatory material except those which would reveal the identity of the source. The intent that this exemption is to be greatly limited can be seen in a colloquy between Congressmen Alexander and Erlenborn in a discussion of the language agreed to in the Privacy Act by the House and Senate:

"Mr. ALEXANDER. In some instances, I suppose, agencies might claim that disclosure of any part of a particular item would reveal the identity, of a confidential source. In those instances, could the agencies conceal even the fact of the item's existence from the citizen who wished to see his file?"

"Mr. ERLENBORN. Absolutely not. The fact that a confidential derogatory statement exists in someone's file, and that the statement could be characterized in some general way, most assuredly would not reveal the identity of a confidential source. The fact of the item's existence and a general characterization of that item would have to be made known to the individual in every case." [17]

While this language may be difficult to apply in every case, it should mark an important turning point in the conduct of background checks and the quality of information gathered for employment and promotion evaluations.

JUSTICE REPORT/PROTECTION OF CITIZENS' PRIVACY BECOMES MAJOR FEDERAL CONCERN

(By Richard E. Cohen)

A concern that government and business accumulate too much data on private citizens is making the protection of individual privacy an issue high on the priority list of scores of government policy makers.

While part of the rush to action is in response to abuses of government power documented in the Watergate scandals, it also is an inevitable result of the rapid growth of government record keeping made possible by the increasingly sophisticated use of computers. A three-year study by the staff of the Senate Judiciary Constitutional Rights Subcommittee revealed the existence of 858 federal data banks containing 1.246 billion separate records of American citizens.

Under the leadership of a White House committee chaired by Gerald R. Ford when he was Vice President, government agencies have been strongly encouraged to deal with a broad variety of privacy invasions. The issues range from the use of medical and employment records to the implications of a "cashless society."

This review of the government's impact on privacy may bear results similar in scope to those generated five years ago by the concern for protecting the environment. And, as with the ecology boom, privacy may be an issue that is easy to support in general terms but raises complex policy and cost questions when the specifics are analyzed. Action also has been frustrated by bureaucraic inertia in many federal agencies.

One result has been a difficulty in securing agreement on legislation whose goals both congressional and executive branch officials say they support but whose provisions may affect a gamut of unrelated areas.

And some Members of Congress who have been in the forefront of the privacy movement have begun to question the motives of the Administration initiative, wondering whether it is designed primarily to serve the White House's political interests rather than to buckle down on agency abuses.

Background: Until about a year ago, privacy was an issue that drew scant public or congressional attention. A few Members of Congress used their committee leadership posts to hold hearings on subjects such as wiretapping and other electronic eavesdropping, consumer credit practices, and the use of lie detector tests. Widespread fear about the creation of a "national data bank" arose in the mid-1960s, but faded after the glare of publicity shined on the proposal.

---

[17] 120 Cong. Rec. H. 12247 (Dec. 18, 1974).

Without any discussion of policy or attempt to set operating standards, the steady growth of federal data banks continued unabated. The only guidelines on federal computer use came from the Office of Management and Budget and the General Services Administration who were interested primarily in procurement practices.

The abuses of individual liberties documented by Watergate have dramatically changed that picture.

"Watergate has made it easier to get the interest and votes of other Members of Congress on privacy issues because they are concerned about the 'plumbers unit' and the use of Internal Revenue Service records, and are responding to it," said Rep. William S. Moorhead, D-Pa., chairman of the Foreign Operations and Government Information Subcommittee of the Government Operations Committee.

"There was a crisis for the past few years in communications and data collection. It took awhile for the counterforce to catch up, but, Watergate made people more receptive to the issue of what the government is collecting," said Henry Goldberg, general counsel for the White House Office of Telecommunications Policy.

Coincidentally, the Member of Congress with the longest and most active interest in privacy regulation is Sen. Sam J. Ervin Jr., D-N.C., chairman of the Senate Select Committee on Presidential Campaign Activities, which uncovered many of the Watergate abuses. As chairman of the Senate Government Operations Committee and the Judiciary Subcommittee on Constitutional Rights, he has been in a unique legislative position to secure privavy legislation prior to his retirement at the end of 1974.

Ervin's two principal bills are designed to regulate the use of criminal history information and provide rules for the gathering and disclosing of non-criminal information by government agencies. His position as a principal nemesis of the Nixon White House and Justice Department added political complications to the passage of those bills, but his staff has intensified efforts on each of them since the resignation of President Nixon.

FORD COMMITTEE

Acting to anticipate further danger to civil liberties posed by the pervasiveness of government has proved to be a task easier said than done. A few legislative and administrative steps already have been taken, with increased intensity since the Aug. 9 resignation of Nixon, but many problems will continue to be studied while a growing corps of government privacy experts attempts to set more definite standards for identifying privacy problems and providing solutions.

Until seven months ago, the executive branch lacked an identifiable individual or institutional leader to study privacy issues and coordinate proposed initiatives. Responding to the increasing public interest in privacy, President Nixon Feb. 23 created the Domestic Council Committee on the Right of Privacy and named then Vice President Ford as its chairman.

Geoffrey C. Shepard, associate director of the Domestic Council and the initial coordinator of the privacy committee concept, said following its creation that the committee "will not establish a broad philosophy but will produce a series of recommendations and actions that pursue the theme of restricting the government's demand of information from individuals."

Ford, who demonstrated little interest in the privacy issue during his 25 years in the House, seized the opportunity and appointed his own staff to run the committee. He soon had the committee studying more than a dozen areas and he made several speeches focusing on the need for government action to protect privacy.

In a June 26 speech to the National Broadcast Editorial Association, Vice President Ford said "the problem of insuring personal privacy in a computerized society which threatens to open the most personal affairs of each of us to anyone with access to computer-stored information" is one of the "most serious" and "least realized" problems facing the nation.

In the committee's early months, Ford succeeded in having President Nixon rescind an executive order permitting the Agriculture Department to review the income tax returns of farmers and strongly criticized a General Services Administration (GSA) plan to develop a data network with the capability of linking federal agencies. The GSA plan was subsequently shelved by Administrator

Arthur F. Sampson. (*For background on the GSA "Fednet" proposal, see Vol. 6, No. 23, p. 856.*)

Committee operations: In addition to the Vice President, Nixon appointed six Cabinet members and four sub-Cabinet officials to the committee and asked the committee to give him "a series of direct, enforceable measures" within four months. The committee members included the Secretaries of Treasury, Defense, Commerce, Labor and HEW, the Attorney General, the chairman of the Civil Service Commission, and directors of the Office of Management and Budget, Office of Telecommunications Policy and Office of Consumer Affairs.

The committee held its first meeting at the White House Feb. 26, three days following Nixon's nationwide radio address. According to Shepard, Nixon attended 70 per cent of the two-hour meeting and told the group the government collects too much information that it has no reason to have and cannot use.

Initial activity—Ford appointed Philip W. Buchen, his close friend and former Grand Rapids law partner, as the committee's executive director. It was the first significant government post for Buchen, who Ford named his counsel shortly after he became President.

With the assistance of a staff of three professionals, Buchen supervised the selection of the committee's initial targets. Task forces were established containing representatives of the agencies involved in a specific problem area. The task forces were told to meet as often aspossible in order to develop firm Administration policy in the 14 areas initially identified by the staff and endorsed by the committee.

Although the committee members did not meet again until July 10, and have not met since then, the committee's over-all progress is reviewed once every three or four weeks by a "liaison group" of assistants to the 11 committee members.

According to Carole W. Parsons, a committee staff member, the existence of the committee, its creation of task forces and the elevation of its first chairman to the presidency have caused "agencies all over the executive branch to take notice of the privacy issue and begin to address it." She estimated 200 to 300 persons are directly involved in committee projects.

Douglas W. Metz, deputy executive director of the committee and the principal staff officer since Buchen became counsel to the president, said the committee views its role as providing "leadership in the implementation and coordination of the initiatives which it has endorsed."

One agency official, who is familiar with the work of the committee, said it has been handicapped because its small staff has had to rely heavily on the agencies whose policies are being reviewed. "The big difficulty has been the lack of aggressive leadership from Mr. Ford, who has not had enough time, and Mr. Buchen who has been understandably cautious because he is not an expert on these issues."

OMB role—While the Domestic Council committee developed initiatives and supervised the task forces seeking to find solutions to the problems, the Office of Management and Budget played a key role in coordinating the increased executive branch activity on a number of privacy issues.

Robert H. Marik, OMB associate director for management and operations, played down the importance of Watergate as an explanation for the accelerated government interest in privacy regulation. He attributed the increased interest to a July 1973 report of the HEW Department's Advisory Committee on Automated Personal Data Systems.

That study, initiated in 1972 by HEW Secretary (1970–73) Elliot L. Richardson, was the first significant departmental review of the implications of government computer technology and it contained a number of recommendations designed to ensure personal privacy. (For a review of the HEW report, see Vol. 5, No. 43, p. 1602.)

According to Marik, who was HEW assistant secretary for administration and management before he joined OMB in February 1974, "We saw at HEW that it was not possible for only HEW to set privacy rules because we were only one part of the federal family, so we searched for a central government vehicle to which all federal agencies could relate, but we could not find it."

Nixon's establishment of the Domestic Council committee provided the vehicle for coordinating new policies. OMB's traditional role of serving as a clearinghouse for agency views on proposed legislative and administrative action, Marik said, "placed us in the position of reflecting the attitude that we walk before we run.

"We know some changes must be made in government use of information but the operation of the data systems is a very costly and sophisticated process. To impose on the process significant regulations is a major undertaking."

Walter W. Haase, OMB deputy associate director for information systems and a principal assistant to Marik, has participated actively in the development of many Domestic Council committee initiatives. He said the creation of the committee was an important step in providing an organization with lead responsibility for privacy concerns within the executive branch and a focal point to carry out President Ford's privacy interests.

He said OMB complements the committee's efforts in coordinating an Administration position by balancing the privacy concerns with other factors such as budgetary considerations and statutory obligations of the agencies.

New president—At its July 10 meeting the Domestic Council committee formally recommended action in 14 areas. Vice President Ford prepared a report for the President on the committee's proposals. Nixon did not discuss the matter with Ford in the next month and on Aug. 9, Ford found the recommendations still resting on "the president's desk." Since then, the committee has operated on the assumption that the 14 initiatives represent presidential policy.

When Ford announced Aug. 20 his nomination of Nelson A. Rockefeller as Vice President, he said that one of Rockefeller's duties, if confirmed by Congress, would be to serve as chairman of the privacy committee. Rockefeller would be expected to bring his own brand of leadership to the committee and perhaps modify some of its earlier actions.

Douglas Metz, currently the committee's operations director, said he favored a more formal structure for the committee outside the confines of the Domestic Council. Metz reviews the progress of the committee's work regularly with Geoffrey Shepard of the council and its executive director, Kenneth R. Cole, Jr. Metz said the committee also needed more resources and staff capability.

In the interim, the committee staff and task forces have been working actively on the implementation of the 14 initiatives, and have added eight new ones.

Early initiatives: Ford chaired the July 10 privacy committee meeting, which endorsed progress on eight intra-executive branch proposals. Although several of the proposals have been or are likely to be the subject of congressional concern, action on these initiatives is designed to lead only to administrative rather than statutory action.

Privacy impact statements—OMB is directing the preparation of a circular with criteria for agencies to use in developing or acquiring new data systems or capabilities. The objective of the initiative is to ensure that personal privacy rights receive "systematic consideration" in the planning of data systems, including the filing of "privacy impact statements" for public inspection 30 days before starting the design and procurement of the new system.

Haase said acceptance of the proposal would result in "an evaluation of the privacy implications of proposed systems at each stage of the development process." OMB has set November as a target for adoption of the circular throughout the executive branch.

A draft copy of the circular obtained by *NJR* includes a requirement that each federal agency establish an "office of record for privacy safeguard plans" which will determine whether proposed systems meet the applicable principles for data systems.

Confidentiality standards—The National Bureau of Standards is directing a study to develop standards for the use of sensitive data and will match these to the security safeguards and economics of computer technology. The study is scheduled to be completed in April 1975.

Although several legislative bills already have proposed a comparable set of standards, as have some executive branch proposals, the study is an attempt to bridge the gap between policy makers and the technicians who eventually will be responsible for ensuring the proper enforcement of new laws.

Consumer transactions—The Office of Consumer Affairs, directed by Virginia H. Knauer, has prepared a "fair information user code" for which it is seeking the voluntary endorsement of a cross section of businesses. The standards are designed to set principles for protecting in the marketplace the privacy of personal information.

Subscribers to the code would "pledge to be responsive" to seven principles, including:

To collect only necessary information;

To use only legitimate methods to obtain such information;

To take reasonable steps to assure that the information is reliable;

To inform the consumer what general uses may be made of the information.

S. John Byington, deputy director of the office, said there would be no enforcement power to the code, but "this does not mean the public or Congress or Federal Trade Commission can't ask a business what it has done to meet the code standards."

He said a draft of the code has been circulated among 15 major companies for their comments, and 10 to 12 of them dealing in retailing, credit reporting, insurance, consumer finance and credit cards have looked at the proposed code in an "agreeable way."

Cable television—The Cabinet Committee on Cable Communications recommended proposals in January 1974 for federal regulation of cable television. The legislation has been under study at the White House since then.

The privacy committee recommended that the Administration proposal include a section prohibiting cable operators from disclosing personally identifiable information about a cable subscriber without his consent or a court order.

Henry Goldberg, general counsel of the Office of Telecommunications Policy, said the draft bill includes comparable language. He added that the only agency holding up final action on the bill by the White House is the Federal Communications Commission, but that he is hopeful a bill can be referred to Congress within a month.

Mailing lists—OMB is directing a study of the use of mailing lists by the federal government. Pending the conclusion of the study, Haase said OMB hopes to issue in the next month an interim policy giving citizens the option of preventing their names from being added to new federal mailing lists.

The Treasury Department recently won its appeal of a case in the U.S. Circuit Court of Appeals for the District of Columbia in which it challenged the right of a manufacturer of winemaking equipment to have access to a Treasury list of all businesses authorized to process 200 gallons of wine each year.

Tax returns—Increased concern about the confidentiality of tax returns, particularly following revelation of White House use of Internal Revenue Service files to attack its "enemies," led the Treasury Department to tighten its rules on records access.

A key step in this process was President Ford's Sept. 20 executive order permitting inspection of IRS records only by the President or his aides upon written request signed by the President. In addition, Treasury prepared legislation setting more formal rules for access to IRS returns by other government agencies.

Sen. Lowell P. Weicker, Jr., R-Conn., and Rep. Jerry Litton, D-Mo., authors of legislation (S 3982, HR 16602) to protect the confidentiality of tax returns, said presidential accessibility to tax returns, "is better preserved by statute than left to the unpredictable course of an executive order." They also have indicated dissatisfaction with the proposed Treasury Department bill. "The Administration bill is full of loopholes," said Litton.

Public queries—OMB has prepared an executive order for President Ford setting agency procedures to assure citizens the right to discover what information the government is collecting about them. Broader legislation in this area has been approved by the House and Senate Government Operations Committees and should a bill be enacted this year, it would vitiate the initiative.

Electronic funds transfer—The Commerce Department, with assistance from banking agencies including the Federal Reserve Board, Federal Home Loan Bank Board and the Treasury Department and the Office of Telecommunications Policy, is studying the implications of movement in the financial community toward a "cashless society."

In the past, federal policy has encouraged experimentation with electronic funds transfer but there has been no study of the potentially significant impact this would have on privacy as a result of the accumulation of large centralized dossiers of personal financial data.

Legislative initiatives: Six of the privacy committee's original initiatives were in response to bills already introduced in Congress. The committee staff has served both to monitor congressional developments and stimulate federal agencies to prepare proposals responsive to the legislative concerns.

Privacy standards—The legislation that has attracted the most interest in both Congress and the executive branch is a proposal stating general guidelines for agencies on the collection and use of data and providing citizens with a number of rights to ensure the accuracy and confidentiality of the records.

Separate bills (HR 16373, S 3418) have been cleared by the House and Senate Government Operations Committee and floor action is considered likely on each prior to the final adjournment of Congress. Both the privacy committee and OMB staff have met formally and informally with congressional staffers in order to resolve conflicting views. They voice greater approval of the House committee bill, calling S 3418 a "drafting horror" and "over broad."

A staff lawyer on the Senate Government Operations Committee said that the committee has not received satisfactory assistance from the White House in the preparation of its bill. "We invited their participation all the way down the line, but they didn't think we were serious about the bill. As a result, their responses have not been comprehensive or the kind of in-depth analysis we would like to see," he said.

Military surveillance—The Senate Subcommittee on Constitutional Rights has reported to the Judiciary Committee S 2318, a bill prohibiting the armed forces from conducting surveillance of civilians. The privacy committee recommended passage of an "acceptable revision" of the bill.

The Defense Department, which had earlier submitted views in opposition to the bill, was designated as the agency to implement the initiative. A Pentagon attorney said "there has been some change in the position of both sides but no meeting of the minds."

Since the subcommittee held its hearings in 1971 on military surveillance practices, the Defense Department has issued department regulations ending its domestic intelligence operations, but the subcommittee believes permanent legislation is needed to forestall changes in executive policy.

Federal employees—The Civil Service Commission has been designated as the lead agency for preparing legislation to protect the privacy of civilian employees of the executive branch.

The matter has been the subject of legislation sponsored by Sen. Ervin and passed by the Senate on several occasions in the past decade but with no final House action. The bill's provisions have included a ban on the use of polygraph tests for federal employees and prohibition of practices forcing employees to buy bonds or disclose their assets. The most recent Senate action on the proposal was passage of S 1688 on March 7.

In the House, the Post Office and Civil Service Committee has had a comparable bill pending for several weeks. The House draft is weaker than the Senate bill because it would exempt additional agencies and remove the right of counsel.

Donald F. Terry, staff director and counsel for the Subcommittee on Retirement and Employee Benefits of the Post Office and Civil Service Committee said the Civil Service Commission has not softened its opposition to the tougher sections of the Senate bill in spite of the privacy committee's initiative. He said that Anthony L. Mondello, general counsel of the commission, and Douglas Metz of the privacy committee approached him a month ago with a draft bill outlining the Administration's position representing "no real change."

School records—The one legislative initiative that has been enacted is a provision calling for the protection of the privacy of school records. The committee announced its support for an amendment to the 1974 elementary and secondary education bill sponsored by Sen. James L. Buckley, Con-R.-N.Y. The provision requires schools and colleges obtaining federal funds to give parents and college students the right to inspect pupils' school records and to limit further disclosure.

As signed into law (88 Stat 484) by President Ford, the so-called Buckley amendment guarantees access to school records by parents and college students, and limits access by third parties that do not have parent or student consent. John D. Kwapisz, legislative assistant to Buckley, said the privacy committee "played no great role but lent moral support" to passage of the amendment. The HEW Department continued its strong opposition to the amendment in spite of the privacy committee's position.

Bank secrecy—The Treasury Department has been assigned the responsibility for drafting legislation to protect the confidentiality of bank transactions. It is not likely that the bill will be completed before the end of this Congress.

Sen. Alan Cranston, D-Calif., has proposed S 2200, which would impose a ban on most practices of financial institutions giving their customer records to federal agencies. The privacy committee announced its support of that "basic concept" but according to a staff member of the Senate Banking, Housing and Urban Affairs Committee, the provision is "violently opposed" by the Internal Revenue Service and FBI.

Fair credit reporting—Congress enacted in 1970 the Fair Credit Reporting Act (84 Stat 1128) regulating the activities of consumer reporting agencies. Sen. William Proxmire, D-Wis., the principal sponsor of the act, has filed S 2360, which would require additional disclosure of information by credit agencies and right of access by consumers. Following hearings last year, the bill was tabled 4–2 by the Senate Banking Subcommittee on Consumer Credit. However, Proxmire is expected to push for action again when he becomes banking committee chairman next year.

The privacy committee designated the Office of Consumer Affairs to develop an alternative to S 2360. A task force, headed by John Byington, has completed its report and sent it to the committee for further action. Among its recommendations are a modification of the current exemption for medical records.

New initiatives: Since the July 10 meeting, the privacy committee staff and liaisons have studied eight additional initiatives, many of which are still in the planning stages.

Social Security number—Increased use of the social security number as an identifier by both government and private agencies is one of the most controversial and publicly discussed privacy issues.

A task force has been established under the direction of the HEW Department to study possible limitations on its use. Two principal options of the task force are to permit use of the number if the agency has adopted a fair information practices code, and to authorize that an individual be penalized for not giving a number only where the requester has authority to use it.

David B. H. Martin, who was executive director of the earlier HEW advisory committee on privacy, is preparing a policy paper for proposed HEW action. Once the department adopts a position, it will be reviewed with other federal agencies.

Research data—OMB is supervising a study on the means to protect the confidentiality of data collected strictly for research purposes. According to Carole Parsons of the privacy committee staff, the proposal is designed to "insulate sensitive records from compulsory process." One unresolved question, she said, is the extent of research efforts that should be covered.

Health records—An HEW project has been established to review existing departmental practices on the use of health and medical records, including the keeping of records in compliance with the statutes dealing with medicare, medicaid, and the cost and quality of medical services.

National security—The Defense Department has initiated a study of the suitability investigations by federal agencies to determine whether individuals are qualified for employment, contracts and access to classified information of a national security character.

Social Security Administration—This study by Social Security officials is reviewing the agency's internal fair information practices on the use of Social Security records, not the use by others of the social security numbers.

Employers records—The Labor Department is supervising a study of personal data by private employers in hiring and promotion decisions. J. Michael Taylor, an attorney in the solicitor's office, said the committee will attempt to "balance the employee's right to be left alone with the employer's need to know if the employee is qualified and honest." Among the practices to be studied are use of arrest records, lie detector tests, insurance records and credit reports.

Information collection—The privacy committee staff is formulating a study of the amount and type of information that is collected by federal agencies. According to Ms. Parsons, "this is one of the most difficult issues to get a handle on, and we're not sure how to proceed."

The subject is of special interest to small businesses which have complained about excessive federal reporting procedures. The House Oct. 7 approved without dissent HR 16424, a bill to establish a Commission on Federal Paper Work to study similar problems.

Privacy R&D—The committee staff is also considering proposals to encourage research programs on privacy issues by federal agencies, and to designate a federal office to make known the government's interest in the subject to private researchers.

PRIVACY STANDARDS

The most significant action on privacy legislation by Congress this year is likely to be enactment of a bill setting general standards for federal use of citizens' records in its data banks. The legislation has been referred to as a federal "fair information practices code."

The principal features of the bill are likely to be guidelines requiring that, with respect to most federally operated data banks:

The information not be disseminated to another agency without the written consent of each individual whose record would be transferred;

The record be accurate, relevant and timely;

The individual know of the record, have access to it, and be permitted to request a correction when he claims there is a mistake, with an ultimate right of court review;

Civil penalties be available to the individual in case of government violation of the regulations.

Whether the 93rd Congress will enact a privacy bill will essentially be a question of time. Supporters of the proposal in each chamber attempted to have the House and Senate consider the separate bills prior to the scheduled Oct. 11 start of the election recess. The bills are sufficiently complicated and the differences between them are such that a conference committee will almost assuredly be necessary.

Assuming the congressional leadership adheres to its current plan of a post-election session, there probably would be enough time for the conferees to resolve the differences between the two chambers and send the agreement to President Ford prior to final adjournment. If Congress does not pass a bill, Ford's aides say he will issue an executive order containing many of the proposed actions.

House: The Government Operations Committee Sept. 24 approved without dissent HR 16373, the Privacy Act of 1974. The bill was drafted over a period of several months by the Foreign Operations and Government Information Subcommittee, chaired by Rep. Moorhead, with considerable assistance from the two ranking subcommittee Republicans, Reps. John N. Erlenborn of Illinois and Paul N. McCloskey Jr. of California.

The bill, which has as its principal aim the limitation of the use of personal records by the government, was drafted as an amendment to the Freedom of Information Act of 1966 (80 Stat. 383). Ironically, that law is designed to encourage the government to make public more information. Norman G. Cornish, the subcommittee's deputy staff director, explained that the drafting decision was made on the basis that the 1966 law is the only current federal law dealing with information practices.

According to the committee's report accompanying the bill, the legislation "recognizes the legitimate need of the federal government to collect, store, use and share among various agencies certain types of personal data" but provides safeguards to remedy misuse of the information and "reassert the fundamental rights of personal privacy of all Americans."

The keystone to the bill is that, with limited exceptions, a federal agency cannot divulge to another agency personal information about an individual without his consent. Among the exceptions are the activities of law enforcement agencies, the Census Bureau's official surveys, emergency situations and information needed by Congress for legislative and investigative reasons.

In an interview, Rep. Erlenborn said the bill is important because "technology has progressed to the point where a government agency can push a button and get a mass of information on almost anyone. There should be an assurance that the information is used only for the purpose for which it was collected." He added that while there have been some abuses in the past, passage of the bill is necessary primarily because of "a fear of the future."

Cornish said that "for the first time in the country's history, Americans will have some control over how the federal government utilizes information concerning them and can ensure that the information is used by the government only for the purpose for which it was knowingly submitted."

White House assistance—The drafting of HR 16373 was noteworthy for what all sides acknowledged was a substantial and generally amicable contribution by President Ford's privacy committee and the Office of Management and Budget.

Subcommittee Chairman Moorhead said: "We don't want to interfere with good management of government. The privacy committee staff and OMB were helpful to us and we resolved a number of issues with them." Erlenborn said he had "never seen better cooperation" between OMB and a congressional committee on the drafting of legislation.

OMB Associate Director Marik said there was a "magnificent working relationship" between the subcommittee and the White House, and that the subcommittee

was "very responsive" to the points made by OMB. With the exception of one section, he said he supported enactment. Metz of the privacy committee expressed similar views.

Federal employees—The principal outstanding point of contention between the subcommittee and the White House is whether the bill should be applicable to the records of federal employees and whether, for example, they should be entitled to review their employment records.

During the committee debate, Erlenborn said that unless the exemption were adopted, "the bill will wipe out the confidentiality of the civil service system and compromise the commission's testing process." Rep. Dante B. Fascell, D-Fla., responded that "case after case has shown that you can't get to the root of why an individual employee is not qualified without access to his records." The committee rejected Erlenborn's amendment to add the federal employees exemption by an 11-22 vote.

One controversial section that was struck from the House subcommittee bill would have permitted court awarding of punitive damages against the government in case of a violation of the act. The bill's principal supporters conceded that such a provision would likely provide an unprecedented citizen remedy against the government but argued that it was a necessary "club" against the government.

Senate: The Senate Government Operations Committee Aug. 20 unanimously approved S. 3418. Although much of the bill is structured similar to HR 16373, the drafting process has been considerably more strenuous and has lacked the cooperation with the Administration that marked the House action.

The committee's report is more critical of current government abuses of privacy than is the House committee report. "The lack of self-restraint" by some agencies "has demonstrated the potential throughout government for imposing coercive information burdens on citizens or for invading areas of thought, belief or personal life which should be beyond the reach of the federal data collector," the report said.

The bill, introduced by Chairman Ervin and co-sponsored by Sens. Edmund S. Muskie, D-Maine, and Charles H. Percy, R-Ill., had three days of hearings in June and the one committee markup session in August. In both cases, the House committee gave the bill significantly more lengthy attention.

Criticism—According to several Administration critics of the bill, this quick action reflected the bill's vagueness and inadequate attention to specifics. One White House aide said "there is a genuine commitment among Senators to the bill, but the problem is that the bill needs considerable tightening."

A private attorney who observed the committee's markup session and did not wish to speak for attribution said: "I had a strong feeling that the Senators and staff did not understand the bill and its implications." He said that he sympathized with the staff because of the "enormously complex problems" and suggested that legislation may not now be the answer to the privacy concern.

Lawrence M. Baskir, chief counsel and staff director of Ervin's Constitutional Rights Subcommittee, who participated in the drafting of the bill, disagreed that S. 3418 was more unusual or complex than other legislation approved by Congress. "All of the proposals in the bill have been discussed since at least 1970. Our staff is very familiar with them and has been working on privacy longer than anyone in the executive branch," he said.

He was particularly critical of what he called "last minute quibbling suggestions" from the White House. "The executive branch is good in suggesting changes but it still has not prepared its final position even though the bill has been pending for several months," he said Sept. 25.

A 35-page memo commenting on the bill was sent Sept. 16 to the Government Operations Committee staff by Metz. Two days later, the committee received a seven-page listing of "major concerns" from OMB Director Roy L. Ash.

Commission—A principal point of dispute in S. 3418 is its proposal to establish a Privacy Protection Commission as an independent agency. Its purpose would be two-fold—to adopt guidelines to assist government agencies in implementing the acts, and study federal data bank practices and recommend necessary changes to Congress and the President.

James Davidson, counsel to Muskie's intergovernmental relations subcommittee, said the commission is necessary because of both the need for a central point of expertise in implementing privacy rules and the fact that there has never been a full-fledged study of privacy problems in both the public and private sectors.

The White House response to the Senate committee is that the commission would be "another layer of bureaucracy" that would slow the initiation of the new regulations, and might also be "a handy excuse for delaying the implementation of some important privacy safeguards."

White House: In the event that the House and Senate do not reach agreement on a federal privacy standards bill before the 93rd Congress finishes its work, President Ford will issue an executive order modeled on the standards of the pending legislation.

Metz said the executive order would be "nearly identical" to the House committee bill. "We are committed to action—either executive or legislative—to show the good faith of the Administration to act."

Metz said there was no White House preference for an executive order instead of legislation and that Ford and his aides will continue to push for a bill until it is clear that there is "no opportunity for legislative action in this Congress."

Baskir, Ervin's chief aide on privacy legislation, criticized the White House for having an executive order ready to be issued in lieu of the legislation. He said this and the "last-minute criticisms" of S. 3418 led him and others in Congress to believe "the Administration position on privacy is to cooperate but still obstruct progress in order to prevent the bill from being passed."

The result, he said, would be that the Democratic Congress would pass no privacy legislation and the President could issue his own executive order and "steal the thunder."

Baskir's contention was denied by OMB's Marik who said Ford's intentions are "genuine."

ASSESSMENT

A review of privacy developments during the first nine months of 1974 demonstrates the involvement of a substantial number of executive and congressional officials in the struggle to develop regulations to deal with the real and potential threats to individual liberties posed by the growth of computer technology.

President Ford has several times since he became President referred to his abiding interest in the privacy issue and he gives every indication that he intends to keep the issue alive. Nelson Rockefeller may give new direction to the White House privacy committee but it is probably too late to move it in the direction of less activity rather than more.

Key questions remain, however, as to the extent to which the White House can and will attempt to budge the often recalcitrant agencies from their traditional positions of adhering to "tried and true" bureaucratic practices.

There is also the question as to the extent Ford is willing to share the privacy limelight with Congress.

Rep. Litton of Missouri, a principal supporter of greater confidentiality of tax returns, said Ford and Buchen were extremely interested in his proposal during the summer. This changed after Ford became President, Litton said.

"The more they looked at the issues, the more they realized it wasn't so easy as they thought, and the pressure from the agencies got to them," he said.

Norman Cornish of the House Government Operations Committee staff emphasized that OMB and the White House were cooperative with his committee in trying to work out legislative problems.

But he said "the Administration inclination to turn to executive orders is a bad omen" of a possible lack of full cooperation between the President and Congress.

Whichever way the initiatives and working relationships turn, officials at both ends of Pennsylvania Avenue agree that privacy will remain a live issue in the post-Watergate climate and that bureaucrats in every part of the government will have to adjust their practices on the handling of citizen records.

They also indicate that the results of the federal privacy regulation program will help dictate future regulation of privately operated data banks. OMB associate director Marik said "the privacy concerns on federal data systems are certainly applicable in the private sector," but added that the federal government should first "put its own house in order and determine the impact of the regulations so that the private sector is not impaired by costly or cumbersome proposals."

Supporters Find Drafting of Criminal Files Proposal a Path Filled With Bottlenecks and Complex Issues

Securing agreement on a bill to regulate the use of FBI criminal history records has consumed thousands of hours of attention from congressional, White House and Justice Department officials and staff. But most participants agree that they are no closer to passage of a meaningful bill than they were a year ago when they began the agonizing effort. They may even be farther apart as a result of the greater understanding of the issues which they have gained.

The drafting process also has been a victim of the Watergate scandal which brought a new Attorney General and Deputy Attorney General who did not feel themselves bound to the earlier Justice Department position on the key issues, consumed the time and attention of the Senator with the most ardent interest in the bill, and made it impossible for the House Judiciary Committee and its staff to consider the proposal during the past six months.

The legislation (S. 2963, S. 2964, H.R. 9783) is designed to set the first national rules on the use and dissemination of criminal justice information and impose restrictions on the exchange of criminal records between the Federal Bureau of Investigation (FBI) and thousands of police departments across the country. Interest in the bill was aroused by the absence of specific laws on the subject, leading many critics to cite a serious threat to personal privacy. (For background on the controversy and details of the proposals, see Vol. 5, No. 43, p. 1599, and Vol. 6, No. 7, p. 246.)

Negotiations: The effort to move ahead on the legislation has been marked by a continual series of meetings between congressional and Justice Department staff, attempts to put on paper what tentatively was agreed to orally, and renegotiations of supposedly final provisions.

"When the crunch comes, the Justice Department is not making decisions, and the White House is not there to push it along. Either the Administration's concern for privacy is a 'paper tiger' or there is a calculated effort to stymie action. In either case, there would be the same result of Congress's inability to act," said Lawrence M. Baskir, chief counsel and staff director of the Senate Judiciary Subcommittee on Constitutional Rights, chaired by Sen. Sam. J. Ervin Jr., D-N.C. (Baskir plans to resign soon and become general counsel of the Presidential Clemency Board.)

Deputy Attorney General Laurence H. Silberman, who has headed the Justice Department's review of the bill since his March confirmation by the Senate, disagreed with Baskir. "We have been working hard for the past month to reach an Administration position. With President Ford's accession to the presidency, the issue became of greater importance, and it became possible to get an administration position. That was difficult under President Nixon because an attempt was tried earlier and it failed."

Silberman was referring to the drafting last fall of the original Justice Department bill (S. 2964) under the direction of Associate Deputy Attorney General (1973–74) Martin B. Danziger. The bill was sent to Congress as a "Justice Department bill" because of the inability to resolve opposition of several agencies, including the Civil Service Commission and Defense and Treasury Departments. Silberman said that the recent review of the bill has resulted in a change in the Justice Department's position in S. 2964.

Staff meetings—The first extended discussions on the bill between congressional and Justice Department staff were 60 to 80 hours of meetings in May and June between Mark H. Gitenstein, counsel of the Senate subcommittee, and Mary C. Lawton, deputy assistant attorney general (Office of Legal Counsel).

They redrafted Ervin's bill, S. 2963, in order to make it more amendable to the Justice Department. However, when Ms. Lawton forwarded the proposed compromise to others at Justice, she found "parts of the department were not happy with the result." In an interview, Silberman said she was only giving the congressional aides "technical help" without indicating the Administration's position.

Several weeks later, a delegation of officials from the FBI, led by John B. Hotis, an FBI attorney who serves as its liaison for legislative issues, went to the Senate subcommittee staff with suggested changes on many of the issues that had been earlier discussed. "We were upset, as was Sen. Ervin," said Gitenstein.

Silberman meetings—In an Aug. 15 letter to Silberman, Sens. Ervin and Roman L. Hruska, ranking Republican on the Judiciary Committee, said the

problems with S. 2963 "are not insurmountable" and added "it is incumbent upon the Department to come forward with proposals for changes in this markup." They suggested a task force be created to develop a compromise bill by the first week of September.

Three or four meetings were subsequently held in Silberman's office including representatives of the Senate and House Judiciary Committees, Justice Department, FBI and Douglas W. Metz, deputy executive director of the Domestic Council Committee on the Right of Privacy.

At the same time, Silberman chaired a series of meetings with representatives of federal agencies that opposed the bill. According to informed sources, some of the most vigorous opposition to the bill came from within the Justice Department, including Assistant Attorney General Henry E. Petersen of the Criminal Division.

Following those meetings, Silberman directed Lawton and Hotis to draft a bill reflecting the consensus of views exchanged at the working sessions. They finished that process Sept. 27 and their draft bill was circulated to several Justice Department officials. In the following two weeks, additional department and executive branch meetings were held to review the revised proposal.

Senate bill: At the same time that Justice Department and congressional negotiators were trying to find common ground on the many controversial issues in the legislation, staff members of the Senate Constitutional Rights Subcommittee met regularly to draft a bill acceptable to the subcommittee members.

Gitenstein and J. C. Argetsinger, subcommittee minority counsel, held a series of meetings resulting in a memorandum listing proposed changes, which was sent to Sens. Ervin and Hruska. The differences between Ervin and Hruska are reportedly narrower than those between Ervin and the Justice Department. As a result, there has been tentative staff agreement on a number of amendments to S. 2963, the original Ervin bill, and the Senators are expected to meet and develop new plans for Senate passage this year.

Arrest records—A central issue has been whether police should be permitted to disseminate criminal records which show an arrest but no conviction. S. 2963 would have permitted this practice only in limited circumstances or if the arrest had been pending less than one year. The latest draft of the bill permits use of arrest records if the local law enforcement agency adopts federal minimum standards. One standard permits use of arrest records or criminal histories not resulting in a conviction if the facts of the case "warrant the conclusion that the individual has committed or is about to commit a crime and that the information may be relevant in that act." The test is taken from the 1968 Supreme Court opinion in *Terry* v. *Ohio* permitting police to "stop and frisk" on the basis of "reasonable suspicion."

Dissemination—The original Ervin bill generally permitted non-criminal justice agencies to receive only conviction records. Under the revised bill, they may receive arrest records less than one year old if there has been an indictment and the charges are still actively pending. A report prepared at Ervin's request by the General Accounting Office showed that only 7 per cent of the requests to the FBI for criminal records are made by police prior to an arrest. Ervin said the report "confirms my suspicions" that FBI records are used primarily for licensing and employment in state and local government.

Gitenstein of the Senate subcommittee staff said the report shows the FBI runs the criminal records system but it is used primarily for non-public purposes, demonstrating the need for civilian, court, and prosecutorial agencies to be a part of the system's management. However, an FBI official said "I don't think most people are upset with the way we handle our records."

Enforcement—S. 2963 proposed a federal-state administrative system to enforce the bill, while the Justice Department strongly believes the FBI should continue to run the criminal records files. The subject reportedly is one of those causing the most debate. Silberman said the issue is "one of the most complicated subjects I have ever seen in legislation." Ervin has stressed that enforcement should reflect the "federal nature of criminal records by insuring the states a role in determining policy on their use. The most recent draft of his bill prohibits a federal agency from control of any records other than an index of the criminal files five years after the bill's enactment.

Sealing—The provision in S. 2963 requiring that all records be "sealed" seven years after their original entry to prohibit their further use has been changed to permit the use of an index of the sealed records. The sealed files could be used

by police officials where an individual is subsequently charged with a more serious offense or as the result of a court order.

Intelligence files—Another controversial issue is dissemination of intelligence and investigative information, which includes confidential reports compiled by police officers. The revised Ervin bill has relaxed its previous proposal by permitting the exchange of such information among law enforcement agencies where a "need to know" or "right to know" has been demonstrated by the requestor, or if "rational inferences . . . warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information may be relevant to that act."

House: While the House Judiciary Subcommittee on Civil Rights and Constitutional Rights held hearings on the subject last winter, its members and staff have been so preoccupied with the impeachment inquiry and the confirmation of Nelson A. Rockefeller as vice president that they have not had sufficient time to participate actively in efforts to reach a compromise.

Subcommittee Counsel Alan A. Parker said Chairman Don Edwards, D-Calif., still supports a less complicated bill such as H.R. 188, which he introduced, setting restrictions on use of arrest records.

Rep. Charles E. Wiggins, R-Calif., ranking Republican on the subcommittee, said privacy legislation is a "priority" item for the subcommittee but predicted there would not be time to act before the next Congress convenes. Wiggins has stressed that the bill should not endanger the policeman on the street by depriving him of needed information.

Outlook: Although there is practically no chance that congressional, Justice Department, and administration officials will be able to reach a final agreement this year on legislation to set standards for the use of criminal history records, their efforts this year have made more likely enactment of a proposal by the 94th Congress. Many of the participants in the drafting process privately voiced frustration with the pace of their toils but continued hope for long-term success.

Republicans Prepare Own Agenda

At the same time that the executive branch was studying initiatives to protect individual privacy, a task force on privacy of the House Republican Research Committee prepared its agenda for legislative action.

Task force Chairman Barry M. Goldwater Jr., R-Calif., said "privacy rights have become subservient to concerns of utility and pragmatism." The task force report was intended to increase public awareness of privacy concerns in the hope that specific reforms will be adopted, he said.

Some of the report's recommendations are similar to the initiatives that are being pursued under the direction of the Domestic Council Committee on the Right of Privacy. The similarities include support for greater protection of the privacy of bank records and consumer credit information, and scaling down of government information requirements.

On several issues, the GOP task force proposed steps that would go considerably beyond proposals now being studied by the White committee:

The use of the social security number should be limited to the operation of old-age, survivors, disability insurance and other programs as required by federal law.

No surveillance or wiretapping of any citizen should be permitted without a court order.

Tougher steps should be taken to guarantee the confidentiality of census Bureau information.

Juvenile court records should be disseminated only to officials directly connected with the child's welfare and rehabilitation.

No arrest records without a conviction may be used in a federally-supported computerized system.

A federal "privacy protection agency" should be established to enforce the proposed legislation.

[From the National Journal Reports, Jan. 4, 1975]

Justice Report, New Privacy Law To Have Major Impact on Government Data

(By Richard E. Cohen)

Legislation passed in the closing days of the 93rd Congress provides the first statutory requirement that government record keeping and data bank practices guarantee protection of an individual's right of privacy. Administration spokesmen believe it will have a major impact on the kinds of information the federal government collects.

Although the bill, which was signed into law by President Ford on Dec. 31, falls short of the goals espoused by some privacy advocates in Congress, it represents a beginning to them toward attaining more stringent restrictions, both legislative and judicial.

Supporters compare the emerging state of privacy law with that in the area of "freedom of information," where the first federal law was passed in 1966 (80 Stat 250). That initial law brought a series of citizens' suits to test the outer reaches of its applicability and a 1974 law, passed over Ford's veto, to correct what supporters felt were loopholes in the original law.

The new privacy law will put the burden on citizens to gain the maximum effectiveness from its provisions. Congressional drafters believe its most important section is a requirement that all federal agencies annually publish in the *Federal Register* notice of the existence and character of their records systems, including the categories of individuals on whom records are maintained and the uses to which those records are put.

The drafters dropped from the final bill a section approved by the Senate to establish minimum standards for the handling and processing of personal information in federal data banks. Instead the law will require only that the information be "accurate, relevant and timely" when an agency uses it to determine an individual's rights, benefits and privileges under federal programs. Even that requirement is weakened by a section exempting "routine uses" of the information, such as the maintenance of social security records or the compilation of payroll information by the Treasury Department.

In addition to citizen interest, the impact of the new privacy law will be determined by the extent to which White House policy makers and management experts see that normally recalcitrant agencies change their existing practices to conform with it. The law authorizes the Office of Management and Budget (OMB) to develop guidelines and regulations for implementing it and to provide continuing assistance to the agencies and oversight of them.

One Administration official suggested there may be problems with the law's implementation because "no one has encyclopedic knowledge" about what specifically is required. "Creativity will be needed to make sure agencies continue to operate their data systems with the same speed. They will need good guidance, especially from OMB," he said.

In addition the Domestic Council Committee on the Right to Privacy or, perhaps a new White House office, will continue to coordinate Administration policy on privacy issues. The Committee, which was established by former President Nixon in February 1974, first was headed by then-Vice President Ford and now will be led by Vice President Nelson A. Rockefeller. The committee had prepared privacy regulations which would have been issued by President Ford if the bill had not passed.

FINAL AGREEMENT

A half dozen staff members of the Senate and House Government Operations Committees were the key participants in the negotiations leading to an agreement. Separate privacy bills (S 3418, HR 16373) were passed Nov. 21 by the Senate and House but contained significant differences in emphasis and enforcement. (*For background on privacy legislation, see Vol. 6, No. 41, p. 1521.*)

The more limited House bill, which was drafted in cooperation with White House aides, was considered a "first step" toward preventing government power from invading personal privacy, according to the bill's supporters. "The House bill would establish for the first time a framework for the collection, use, maintenance and disclosure of federal records of American citizens," said Norman G. Cornish, deputy staff director of the House Government Operations Subcommittee on Foreign Operations and Government Information.

The Senate bill raised strong objections from Administration aides who said that much of it was vague and would result in administrative nightmares for bureaucrats. Government Operations Committee aides worked for more than a month to refine and clarify its language after the committee unanimously approved the bill Aug. 20.

The Senate bill exempted fewer agencies than HR 16373, placed a greater responsibility on them for assuring that records were correct and relevant and established a powerful commission to make sure that the bill would be enforced throughout the government.

Settlement.—Because of the technical complexity of the two bills and the difficulty in getting Senators to attend conference meetings, most of the deliberations to resolve the differences were held on the staff level. One unusual factor marking the negotiations was that Sen. Sam J. Ervin Jr., D-N.C., who has been the Senate's leading figure in support of privacy legislation and was ending his Senate career, was represented by James Davidson, counsel to the Intergovernmental Relations Subcommittee, chaired by Sen. Edmund S. Muskie, D-Maine, because Ervin's principal privacy aides either had retired or were busy with other matters.

The staff aides held a series of meetings the first two weeks in December, including one meeting of approximately four hours with the four key congressional principals—Reps. William S. Moorhead, D-Pa., and John N. Erlenborn, R-Ill., ranking members of the House Foreign Operations and Government Information Subcommittee, and Sens. Ervin and Charles H. Percy, R-Ill., ranking members of the Senate Government Operations Committee. The final staff agreement was reached Dec. 16 and the bill was sent to President Ford Dec. 19.

Issues: After an initial stand-off, the Senate staff aides gave way on most of the principal issues dividing the participants—the extent of the government's burden to make sure records are accurate and relevant, exemption of criminal justice and private data banks and establishment of a commission to enforce the new law. OMB officials worked in close coordination with congressional aides in the final negotiations.

Both the House and Senate bills included sections giving citizens a right to see most records about themselves stored by government agencies and a right to challenge any incorrect listing. Each bill also provided a citizen the right to sue for damages in federal court if an agency failed to maintain correct files about him and imposed criminal penalties against federal officials for willful violation of the law.

Applicability.—HR 16373 applied the accuracy and relevance standards to "use" of the records and did not require that standing files be maintained properly. The Senate bill required that whenever a federal official went to a file or placed something in it, the record should be accurate. Also, the House bill gave the agencies flexibility to disclose freely information for a purpose "compatible" with the reason for its collection; the Senate bill did not provide such freedom.

Senate aide Davidson said "we recognize the difficulty in defining how agencies use information, but they should at least provide some standards to allow an individual some control over the information." House aide Cornish said "the government would grind to a halt if there were no exemption for routine use. Our bill is concerned with non-routine transfers but we force the agencies to identify what are the routine uses and make them subject to further challenge."

The final agreement on this section was primarily the House version.

Criminal records.—A key issue splitting the conferees was whether the bill should apply to the collection of records by criminal law enforcement agencies. The House and Senate Judiciary Committees, which had been considering legislation in this area, did not complete action in 1974. (*For a report on criminal records bills, see Vol. 6, No. 41, p. 1528.*)

Because Sen. Ervin, who chaired the Senate Judiciary Subcommittee on Constitutional Rights which considered the criminal records issue, did not want S 3418 to exempt criminal records, it included provisions which would have been interim requirements pending passage of a more comprehensive bill. House subcommittee leaders, however, insisted that House rules required them to yield to the Judiciary Committee on this issue.

The House conferees won their point, with the exception that law enforcement agencies, including the Federal Bureau of Investigation, are required to identify annually all their data banks and the purposes for which they are used.

Private files.—The final agreement deleted two Senate provisions governing the collection of records by businesses.

The first would have permitted a citizen to require a business maintaining a mailing list to remove his name and address from such a list. The second would have prevented a business from discriminating against an individual because he refused to disclose his social security number.

Enforcement.—A major provision of the Senate bill would have established an independent Privacy Protection Commission to develop model guidelines and assist agencies in implementing the law, and to receive and investigate charges of violations and report them to the proper officials. The Senate report said "there is an urgent need for a staff of experts somewhere in government which is sensitive both to the privacy interest of citizens and the informational needs of government and which can furnish expert assistance to both the legislative and executive branches."

House Members opposed the creation of a commission on the basis that it would create an extra layer of bureaucracy and that Congress and the executive branch already have adequate expertise. The Administration also opposed the commission idea preferring an approach which President Ford said "makes federal agencies fully and publicly accountable for legally mandated privacy protections."

The conferees agreed to establish a two-year seven-member Privacy Protection Study Commission (two of the members each to be appointed by the Speaker of the House and President of the Senate) to study issues not dealt with by the bill. The commission would be expected to give much of its attention to problems in state and local government and the private sector.

A former Ervin staff member said that failure to establish an over-all enforcement agency significantly weakened the bill because of the difficulty in depending on existing institutions to uncover improper data banks. He said that it required the objections of several prominent congressional leaders as well as then Vice President Ford to force the General Services Administration (GSA) to drop its plans to develop "FEDNET," a giant computer system linking GSA and the Agriculture Department. (*For details, see Vol. 6, No. 23, p. 856.*)

However, Stephen M. Daniels, Republican aide to the House committee, said publication in the *Federal Register* of the existence of all federal data banks as well as continued oversight by congressional committees, OMB and the press will provide adequate assistance that the law will be enforced.

IMPLEMENTATION

Because the final law does not give the commission enforcement responsibilities, federal agencies will have the primary responsibility for making sure the new privacy requirements are met.

However, the law authorizes OMB to monitor enforcement and assist the agencies and requires each agency to inform OMB and Congress of any proposals to establish or alter any records system.

"We know that several OMB people who have been working on this bill are well motivated and interested in seeing the law enforced," said Davidson. "Their job will be a difficult one and it remains to be seen what they can do to enforce the law."

Monitoring.—Walter W. Haase, OMB deputy associate director for information systems, said OMB will attempt to establish "interpretive criteria" for the agencies. "Our main theme will be to place on the agencies the responsibility for enforcement and make sure that the rules for the data systems are debated publicly. OMB would act only in an exceptional case."

He said that this role would be consistent with OMB's effort of holding agencies accountable for their actions and intervening "in the event something goes amiss."

Conflicts.—Administration and congressional aides said enforcement of the new law will conflict with the purpose of several other federal laws and practices designed to promote government efficiency and could cause strains in the early period of the law's implementation. They listed the following potential areas of conflict:

The Freedom of Information Act (FOIA) mandates that, with certain exceptions, all government records should be available for public inspection. While the new privacy law does not specifically change the FOIA, it prohibits the disclosure of material "which would constitute a clearly unwarranted invasion of

personal privacy" unless that disclosure would be required by the FOIA under current court interpretations.

The Federal Reports Act of 1942 (56 Stat 1078) attempts to minimize the federal paperwork burden on businesses by permitting government agencies to exchange among themselves information collected from one source for different purposes.

In recent years federal agencies determining the impact of social legislation have increasingly conducted studies using personal data to evaluate the programs' effectiveness.

There has been a trend toward consolidating information, both within an agency and among several agencies, in the interest of efficiency.

According to the OMB's Haase, "a lot of balancing will have to be done among these various objectives and concerns, many of which are not crystal clear."

State Units Examine Policies

State and local governments, which hold far more records on citizens than does the federal government, are beginning to examine their policies on the use of the records and the need to protect them from abuse of individual privacy.

At a conference in Washington Dec. 15–17, 150 state and local government representatives discussed the need for state legislation to regulate the general use of data banks, public employees' records and criminal justice information.

The conference was sponsored jointly by the Domestic Council Committee on the Right of Privacy and the Council on State Governments. According to Douglas W. Metz, acting executive director of the White House committee, numerous local officials have expressed an interest in federal privacy programs and their responsibility for protecting the privacy of local records.

J. Keith Dysart, general counsel of the Council of State Governments, said "state governments are awakening to the problems of privacy and want to do something: they recognize that some state programs abuse privacy rights." Several state legislatures will consider broad privacy legislation in 1975, he said.

One mock legislative committee at the conference studied over-all state and local regulation of record keeping and concluded "comprehensive omnibus legislation . . . is necessary." The panel proposed that state legislation bar secret record keeping, compel disclosure of the use of information, permit the viewing and correction of records and safeguard the accuracy and reliability of data. The committee was divided evenly over whether state legislation should cover the private sector.

Two other committees studied the collection of records about public employees and criminals or suspected criminals. Both committees discussed the principles that should apply to the use of such data but made no specific recommendations.

One common point of interest to each group was the financial impact. Willis H. Ware, researcher of the Rand Corp., said "there is no hard data on the costs of privacy protection but it will not come free." He cited estimates by the Office of Management and Budget that the recently passed federal privacy legislation will cost approximately $200 million a year in operational expenses.

[From the National Journal Reports, May 24, 1975]

Justice Report/Agencies Prepare Regulations for Implementing New Privacy Law

(By Richard E. Cohen)

Federal agencies are drafting rules to govern their use of personal data that will bring substantial changes in federal record keeping practices. Government personnel chiefs, data specialists and lawyers are developing the standards in compliance with the Privacy Act of 1974 (88 Stat 1896), designed to guarantee citizens that personal information will be accurate and used only for the purpose for which it was collected.

The drafting process is being coordinated by the Office of Management and Budget (OMB), which already has disseminated a 114 page set of guidelines to the agencies to assist them in meeting the Sept. 27 deadline for the act's implementation. OMB also will review plans formulated by each agency to make sure that all its records systems meet the criteria of the law.

An OMB official who is involved in this process said the agencies will retain the ultimate authority for meeting the law and that the best monitor of agency responsibility is "public scrutiny." OMB, nevertheless, has broad power as keeper of the federal budget to bring reluctant agencies in line with both the spirit and letter of the law. It has designated three agencies with government-wide responsibilities as lead drafters of rules to facilitate and synchronize the implementation process, which began Dec. 31, 1974 when President Ford signed the Privacy Act.

An official of one of these agencies said one result of the new law is that fewer records will be kept by the government, partly because the law carries civil and criminal penalties for federal employees who violate its terms. "People will think twice of the consequences before they put anything into an automated file in order to make sure there is a statutory right," said Sidney Weinstein, assistant commissioner of the automated data and telecommunications service of the General Services Administration (GSA). The law also will affect private businesses and individuals, particularly government contractors, who supply records systems for federal use.

Weinstein and others said one immediate consequence of the law will be that federal officials will destroy millions of records rather than bring them into compliance with the new law when it becomes effective on Sept. 27.

The law was passed in the final days of the 93rd Congress after growing congressional concern that automated record keeping permits far more collection, storage and exchange of information about citizens by the government, which may result in some uses that were not intended or authorized when the citizen originally provided the data. (For background on the law, see Vol. 7, No. 1, p. 20.)

Then-Vice President Ford gave much attention to privacy issues in early 1974 as chairman of the Domestic Council Committee on the Right to Privacy and, as President, he has continued to stress protection of privacy as one means of restoring public confidence in government. (For a report on the Ford Administration's privacy initiatives, see Vol. 6, No. 41, p. 1521.)

OMB ROLE

OMB's role as the lead agency in the implementation of the Privacy Act was mandated by Congess in the law, when it gave the White House office responsibility for developing agency guidelines and regulations and providing continuing assistance and oversight of the agencies.

OMB was assigned this role after Administration and House leaders objected to a Senate proposal that would have established an independent Privacy Protection Commission with advisory and monitoring functions.

The officials who have the responsibility for supervising the implementation are Walter W. Haase, OMB deputy associate director for information systems, and Franklin S. Reeder, an aide to Haase. Both participated in the drafting of the law.

Shortly after the law was enacted, Haase said OMB would give government agencies the prime responsibility for making sure they are in compliance and that OMB would provide "interpretative criteria" to assist them. Because of the magnitude of the law's coverage and the number of federal records systems, OMB determined that direct supervision of the agencies was impossible and that its more realistic role was to "change bureaucratic behavior" through the existing institutions.

Systems identification

An early prerequisite of the law forced the agencies to identify and list all systems of records which they maintain, both manual and computer. The law requires annual publication in the Federal Register of the existence and character of each system of records about citizens, including the name and location of the system, the categories of individuals and records maintained, the uses of the records and agency practices governing storage, access and disposal.

A draft of the OMB guidelines, which is scheduled to be made final in late May, said the public notice requirement is central to achieving one of the law's basic objectives—"fostering agency accountability through a system of public scrutiny." Public notice of the systems is required this year by Sept. 27.

Many federal agencies, particularly Cabinet departments, are identifying all their systems for the first time, and their officials claim it is a lengthy and tedious bureaucratic process. The Senate Judiciary Subcommittee on Constitutional Rights conducted a survey between 1971–74 of all federal data banks of indi-

viduals. Its 1974 report concluded that the 54 agencies surveyed reported 858 data banks with 1.246 billion records on individuals.

Several persons said the new inventory will reveal a far larger number of data banks, partly because the survey is required by law, not by a congressional subcommittee request. One GSA employee, who did not want to be identified, said the Defense Department alone may have as many as 5,000 records systems. It revealed 497 systems in the Senate survey.

Guidelines:

Once the agencies have identified and described each of their records systems, they will have to make sure that the records meet the legal requirements. The rules include details on proper disclosures, accounting of certain disclosures, access by an individual to his own record, assuring the information is "relevant and necessary" to accomplishing an agency purpose and setting rules to protect the confidentiality of the records.

OMB Director James T. Lynn sent a memorandum to each federal agency head March 12, providing them with them the set of proposed guidelines and requesting the agencies to submit to OMB by April 7 their plans for implementing the provisions of the act.

Lynn's memorandum was sent to nearly 100 agencies, approximately half of which had not responded by mid-May. An OMB aide said all but two of the Cabinet departments, which he would not identify, responded close to the April 7 deadline. None of the agency plans has been made available for public inspection.

Haase and Reeder will review each of the plans to get a "feel" of their content and to see whether the agencies need more help. Their intent is to give the agencies some discretion within the parameters of the general interpretive guidelines so that the agencies can meet the special needs of their own records and the different groups they serve.

Routine use

A key factor in the implementation of the act is the extent to which agencies characterize use of the records as "routine." Although the law requires public notice of all systems of records, it permits an agency to exclude records from the other requirements of the law in the event of a "routine use," defined as a use "compatible with the purpose for which it was collected." Agencies are required to give public notice of all "routine uses" of each records system.

The OMB draft guidelines refer to a congressional staff analysis of the law, in describing "routine use":

"This act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks (or) the receipt of information by the Social Security Administration to complete quarterly posting of account. . . . It is, however, intended to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material."

AGENCIES

In addition to issuing guidelines and reviewing agency plans, OMB has designated three agencies to set regulations that will be incorporated into the procedures of all federal agencies. Officials of these three agencies are coordinating their efforts with Haase and Reeder but they have final legal authority to impose many of their rules.

Civil Service

Because of its role as personnel manager of the federal bureaucracy, the Civil Service Commission is rewriting the rules on the types of data that may be kept on federal employees. Since the commission also maintains a file on every federal civilian employee, it will be modifying its own internal procedures.

Gary D. Bearden, director of the Bureau of Manpower Information Systems, said the commission will provide privacy training courses for some employees in all federal agencies and will integrate a privacy concern in all its future management, supervision and data processing courses. The commission also will have a continuing responsibility to make sure that agencies comply with federal personnel rules.

The commission has prepared a 22 step approach for all its bureaus to follow to carry out the law. A background paper said the review of the commission's

file systems "demands the greatest degree of involvement of all organizational components." The Privacy Act exempts from its coverage employee test materials and the source of investigatory records used in employment checks.

GSA

As manager of federal property and records, the General Services Administration has been assigned several roles in supervising the implementation of the Privacy Act.

Equipment use

GSA has supervisory authority for the purchase of all government computers and telecommunications equipment. Sidney Weinstein of the automated data and telecommunications service said GSA is preparing privacy regulations for agency procurement and sharing of such equipment on the basis that "the proper time to tell an agency how to use the equipment is when the system is being designed, not when it is acquired 6 to 12 months later."

GSA Administrator Arthur F. Sampson issued a regulation in 1974 requiring executive branch agencies to submit for its prior approval all new data processing and telecommunications machines in order to ensure they adequately protect citizen privacy.

Contractors

In coordination with the Office of Federal Procurement Policy, an arm of OMB, GSA is setting rules for federal contractors. An OMB aide said Congress applied the Privacy Act to federal contractors in order to prevent agencies from using "laundered" information to avoid the law.

GSA and OMB officials are uncertain about the impact of this section and the number of private firms affected. However, Weinstein said "few businesses yet understand this section and that it will be a significant requirement imposing additional administrative and technical burdens." GSA officials intend to solicit industrial comments before the final contractor rules are made effective in September.

The OMB draft guidelines said the law covers contractor records systems "maintained to support direct management of a federal program by a federal agency" but does not cover a program or activity financed in whole or in part by the federal government but managed by a local government or non-federal agency.

Archives

GSA's National Archives and Records Service sets rules on the storage of all agency records. Under new privacy regulations, agencies will be required to identify for the archives service all records kept in federal records centers and provide GSA a copy of their privacy rules before the service provides them copies of the records. The purpose of this regulation will be to assure that only authorized agencies have access to the records.

The archives service also supervises the Federal Register, which is required to publish the annual notice of federal records systems as well as all new rules governing their use. It is preparing rules governing the format of these notices.

National Bureau of Standards

The Commerce Department's Bureau of Standards recently studied the protection of computer security and is advising agencies on how to prevent inadvertent disclosure intentional misuse, bad data and other problems.

Ruth M. Davis, director of the Institute for Computer Sciences and Technology, is supervising the drafting of regulations that will apply to all federal agencies. Congressional aides said she is concerned that OMB has not given the Bureau of Standards adequate time or funds to implement the act. Davis was not available for comment.

COMPLIANCE

While there is no uniform pattern for implementation of the Privacy Act by individual agencies and it is too early to measure the extent of compliance, many large government departments have created offices setting agency information policy. Some officials have pointed to possible problems and conflicts in implementing the law.

Commerce

James N. Ravlin, special assistant to the Commerce Department general counsel, said the department has begun an inventory of its records systems but

is awaiting the final OMB guidelines before it begins to apply the new rules to the systems and to educate the staff.

Ravlin said the department has discussed with OMB several questions on the law's interpretation including whether it covers persons whose records are kept for requirements, such as equal employment opportunity, having nothing to do with them individually, and those who are references for job applicants.

He also said "there is some inconsistency in the OMB guidelines on how much help an agency should give an individual in locating his record and how specific an agency should be in reporting the purpose of which the record is collected."

Labor

Sofia P. Peters, Labor Department counsel in the division of legislation and legal counsel, said the department is reviewing each of its nearly 20 divisions to identify precisely each of its records systems. Because of the law's broad coverage, she said, records such as federal employee compensation and data on black lung compensation will be available to the individual described.

She said the preliminary response from the divisions indicates "some of the officials don't understand the total problem. In many cases, they have not identified for us records systems about individuals that are not easily retrieveable or catalogued by a person's name." She said one beneficial result of the new law will be more organized record keeping systems.

HEW

The Health, Education and Welfare Department's (HEW) fair information practices office is supervising the implementation of the law throughout the department. Thomas S. McFee, HEW deputy assistant secretary for administration and management, said the act may be too unwieldy if "interpreted literally." As an example, McFee said HEW will not keep a record of each individual access to a record but will maintain records that permit an "audit trail" for anyone seeking such access

HEW prepared the first detailed report on federal record keeping in 1973 when it issued a series of recommendations on computer handling of records, including a proposed "code of fair information practices." Many of the recommendations have served as a guide in subsequent congressional and administrative action. (For a report on the HEW study, see Vol. 5, No. 43, p. 1602.)

Justice

Although the Privacy Act requires public notice of all criminal information systems, it permits an agency to exempt most criminal records from the other procedural requirements of the law. Justice Department and congressional aides have worked for two years on separate legislation governing these files and hope a law will be enacted later this year.

Mary C. Lawton, deputy assistant attorney general (Office of Legal Counsel), told an April 16 meeting of state criminal justice officials that the new law is "bound to impact on local criminal justice agencies," citing their use of records from non-law enforcement agencies.

She said the Justice Department will not apply the act literally "because we have interpreted that Congress is not intending the ludicrous even though the law would permit the ludicrous."

Congressional oversight

Several House and Senate aides who participated in the drafting of the Privacy Act have kept a close watch on its implementation. They are satisfied, for the most part, with OMB's performance but express some concern whether there will be full compliance by Sept. 27.

A group of seven congressional aides met April 29 with Haase and Reeder for more than two hours. "OMB might be doing things in a different way but there is movement that is going in the right direction," said James Davidson, counsel to the Senate Government Operations Subcommittee on Intergovernmental Relations.

He said Haase reported some difficulties with agency compliance but gave them no details.

An OMB official said that 50 of the nearly 100 agencies, including all Cabinet departments, had submitted their plans for compliance by May 12, five weeks after the OMB deadline. He said OMB plans to send a follow-up letter to the other agencies urging prompt compliance.

Joseph A. Overton III, legislative assistant to Rep. Barry M. Goldwater Jr., R-Calif., said Goldwater Jr., R-Calif., said Goldwater is concerned that OMB's

guidelines so far "are more description than proscription." Overton said Haase assured the group that OMB would become increasingly diligent in supervising implementation. Overton also expressed concern that "some agencies have so far responded in a totally unsatisfactory manner," according to the general comments of the OMB officials.

Stephen M. Daniels, assistant minority counsel for the House Government Operations Committee, said OMB is in the best position to "direct the activities" of other government agencies and that its performance so far has been satisfactory. He added that the public will have the ultimate right to take recalcitrant agencies to court.

IMPACT

Most officials interviewed said the new privacy law will have a significant impact on federal record keeping practices. While the act will probably cause a short-term reduction in the amount of records that are kept, it is likely to increase the cost of maintaining them and its procedures will increase the amount of bureaucratic paperwork.

By forcing more organized handling of federal records systems, the long-term effect of the law is likely to be increased computerization and an even greater ability of federal officials to secure access to individual data.

In contrast to the 1966 Freedom of Information Act (80 Stat. 383), which forces an agency to respond only when a citizen asks to view a public document, the Privacy Act places more active responsibility on federal agencies to see that record keeping practices are respected.

Cost estimates of the first year's implementation are uncertain, but they range as high as $300 million with annual costs of $100 million thereafter.

Gary Bearden of the Civil Service Commission said when the law was passed, "there was more fiction than fact" in the agencies about its impact. As they have begun "to put their shoulder to the wheel," he said, agency officials have recognized the need for and practicality of compliance. He said that once the initial operating changes are completed, there will not be a significant impact on agency procedures.

Davidson of the Senate Intergovernmental Relations Subcommittee staff said a key factor in the successful implementation of the law will be whether administrative policy officials rather than technical data processing experts or lawyers with general interest supervise agency enforcement of the law. So far, OMB has preferred to allow each agency to make its own decision on which office is given the enforcement power because of its view that each agency is best equipped to make its own decision.

Calendar for Compliance

The Office of Management and Budget (OMB) has issued a calendar to guide federal agencies in the implementation of the Privacy Act of 1974. OMB officials have said they intend to monitor the plan closely, although they may grant some leeway on everything but the final implementation date, which is manlated by the act. Following are the key dates with which agency officials have been asked to comply:

May 30: OMB issues a circular spelling out the basic policies and responsibilities to be met by the agencies, as well as detailed guidelines on the specific terms of the Privacy Act.

June 1: Civil Service Commission begins to introduce training on privacy practices into its courses for federal employees.

June 1: General Services Administration begins to train agency employees on new records management procedures.

June 15: Agencies complete for OMB the draft version of their public notices of their records systems and rules governing their use.

July 15: Agencies complete their plans for implementing the new law, issue changes, to their internal operating procedures and begin intensive employee training.

Aug. 27: Agencies publish for public comment in the Federal Register their rules for use of records systems and which systems will be exempted from coverage of the law.

Sept. 27: Agencies publish in the Federal Register final rules and guidelines for their records systems and give public notice of all records systems which they maintain, regardless of whether they must be publicly available. The Privacy Act goes into effect.

PRIVACY AND THE FREEDOM OF INFORMATION ACT

Mary Hulett*

The second session of the 93rd Congress devoted substantial attention to bills which would restrict disclosure of government information and others which could require disclosure of the same information. This Congress passed, over the President's veto, amendments to the Freedom of Information Act substantially strengthening the disclosure requirements of that Act.[1] The Congress also considered over 100 privacy bills; the House passed the Moorhead Bill[2] and the Senate passed the Ervin Bill.[3] As a compromise, the Congress passed the Privacy Act of 1974[4] enacted as an amendment to the Moorhead Bill and substituted for the Ervin Bill. While the requirements of privacy and of access are in many ways consistent, there is a point of clear conflict where privacy taken alone would require that personal[5] material held by a government agency never be disclosed and access would require that any material held by a government agency must always be disclosed. Obviously, neither privacy nor access can ever be considered alone; both must be considered in relation to other needs and in relation to each other. Unfortunately, the Congress has not clearly

*Third-year student, the National Law Center, George Washington University.

[1]H.R. 12471 (1974) amending 5 U.S.C. 552 (1966) (hereinafter FOIA and FOIA amendments).

[2]H.R. 16373, Rep. No. 93-1416, 93rd Cong. 2d Sess. (1974) (hereinafter the Moorhead Bill).

[3]S. 3418, Rep. No. 93-1183, 93rd Cong. 2d Sess. (1974) (hereinafter the Ervin Bill).

[4]Pub. L. No. 93-579, 93rd Cong. 2d Sess. (Dec. 31, 1974) (hereinafter The Privacy Act).

[5]Privacy, for the purposes of this paper, refers only to personal privacy of individuals with no consideration whether corporations can claim a right to privacy.

addressed this conflict. The result is conflicting requirements on government agencies and a statutory pattern that does not clearly provide for the needs of either access or privacy.

This conflict is made more real for federal agencies and federal employees faced with making decisions on FOIA requests that include personal information. Agency personnel in a short time period,[6] with inadequate guidelines, are forced to decide whether material is required to be disclosed under FOIA or protected from disclosure under the Privacy Act. The problem is intensified by the possible disciplinary and contempt proceedings, for improper refusal to disclose as required by FOIA.[7] While Senator Ervin asserted that the Privacy Act maintains the status quo with respect to the privacy exemption of the FOIA,[8] an analysis of both Acts does not support that conclusion. The FOIA encouraged agencies to err on the side of disclosure by never forbidding disclosure while the Privacy Act permits disclosure only when it is "required."[9]

RIGHT OF PRIVACY

The greatest difficulty in this area is the ambiguous nature of privacy. While much has been written on the subject, it does not include a clear, working definition. There is agreement on the existence of a constitutional right to privacy,[10] although privacy is not explicitly mentioned in the Constitution. Privacy is a newly emerging constitutional right without clear legal definition.

Non-legal definitions are no more clear. Some definitions are: "The essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared or withheld from others. The right to privacy is, therefore, a positive claim to a status of personal dignity—a claim to freedom, if you will, but freedom of a very special kind."[11] "Privacy is the claim of individuals to determine for themselves when, how,

---

[6] 5 U.S.C. 552 (a)(6)(A) amending 5 U.S.C. 552 (a)(3).

[7] 5 U.S.C. 552 (a)(4)(E) amending 5 U.S.C. 552 (a)(3).

[8] 120 CONG. REC. S 21817 (daily ed. Dec. 17, 1974).

[9] Pub. L. No. 93-579, 5 U.S.C. 552a(b)(2).

[10] Griswold v. Connecticut, 381 U.S. 479, 85 S. Ct. 1678 (1965); Eisenstadt v. Baird, 92 S.Ct. 1029 (1972); Stanley v. Georgia, 394 U.S. 557 (1969); Roe v. Wade, 410 U.S. 113 (1973); Doe v. Bolton, 410 U.S. 179 (1973).

[11] Ruebhausen and Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1189 (1965).

and to what extent information about them is communicated to others."[12] "Privacy is not simply an absence of information about us in the minds of others. Rather it is the control we have over information about ourselves."[13] But none of the definitions address the basic question of what kinds of requests offend personal privacy. The factors that need to be addressed are requests for what kinds of information; who is making the requests, and under what kinds of surrounding circumstances. Few would claim that all requests for disclosures at all times violate personal privacy, but the nature of the parameters of privacy are undefined.

What does seem to be agreed upon is that privacy is not the absence of disclosure but the element of control over the disclosures. This element of control is a two-step process. First, it is the control over whether or not to make the disclosure, and secondly, having made the initial disclosure, control over any further use to be made of the information. Since constitutional rights are in fact only proscriptions against government action, the right of privacy means that the government is limited in its ability to require the individual to give up information about himself and is further limited in what the government might do with that information once given up. These two steps are frequently distinguished as privacy, the collection of the information in the first instance, and confidentiality, the status of the information once collected.

Privacy is not an absolute right, it is a right to be balanced against other needs in an organized society. "The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire."[14] "For any one individual, privacy, as a value, is not absolute or constant; its significance can vary with time, place, age and other circumstances. There is even more variability among groups of individuals. As a social value, furthermore, privacy can easily collide with others, most notably free speech, freedom of the press, and the public's 'right to know.'"[15] In the area of conflict between right of privacy and freedom of the press, Justice Corley has said, "A consideration of the limits of the right of privacy requires the exercise of a nice discrimination between the private right 'to be let alone' and the public right to news and information; there must be a weighing of the private interest as against the public interest."[16]

---

[12] WESTIN, PRIVACY AND FREEDOM 7 (1967).

[13] Fried, *Privacy* 77 YALE L.J 475, 482 (1968).

[14] WESTIN, PRIVACY AND FREEDOM 7 (1967).

[15] *Secretary's Advisory Comm. on Automated Personal Data Systems*, HEW, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS 38 (1973).

[16] Carlisle v. Fawcett Pub. Inc., 20 Cal. Rptr. 405 (Ct. App. 1962).

RIGHT TO KNOW

One of the interests to be balanced against the right of privacy is the interest in an informed citizenry, in the citizen's "right to know." The free flow of information from a government to its citizenry is the "life blood of democracy" and information is the currency of power.[17] The old motto 'And the truth shall make you free' has a critical political application. Although the truth may not, by itself, be quite sufficient to make or keep anyone free, the full and free flow of truthful information is clearly necessary to social and political freedom.[18]

It has been argued that the "right to know" is a constitutional right embodied in and necessary to the right of a free press and the right of free speech.[19] The Supreme Court said in *Grosjean v. American Press Co.*,[20] in reference to freedom of the press, "In the ultimate, an informed and enlightened public opinion was the thing at stake." Any argument for a constitutional right to know includes the words of James Madison, Chairman of the committee which drafted the first amendment, "A popular government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance. And the people who mean to be their own governors, must arm themselves with the power, which knowledge gives."[21]

THE FREEDOM OF INFORMATION ACT AND PRIVACY

Congress recognized the basic idea of a right to know in the passage of the FOIA in 1966. In providing a statutory right of access, a possible conflict with privacy was recognized. The House committee report on the FOIA states: "The right of the individual to be able to find out how his Government is operating can be just as important to him as his right to privacy and his right to confide in his government. This bill strikes a balance considering all these interests."[22] "[I]t is necessary to protect

---

[17]Nader, *Freedom From Information: The Act and the Agencies*, 5 HAR. CIV. REV—CIV. LIB. L. REV. 1 (1970).

[18]MINOR, THE INFORMATION WAR IX (1970).

[19]*See Access to Government Information and the Classification Process—Is There a Right to Know?*, 17 N.Y.L.F. 814 (1971); Kutner, *Freedom of Information: Due Process of the Right to Know*, 18 CATH. LAW. 50 (1972).

[20]297 U.S. 233 (1936).

[21]Letter from James Madison to W.T. Barry, Aug. 4, 1822, in THE COMPLETE MADISON 337 (1953).

[22]SUBCOMM. ON ADMIN. PRACTICE AND PROCEDURE, FREEDOM OF INFORMATION ACT SOURCE BOOK, S. Doc. No. 98-82, 93rd Cong., 2nd Sess. 2 (1974).

certain equally important rights of privacy with respect to certain information. . . . It is also necessary for the very operation of our government to allow it to keep confidential certain material. . . . It is not an easy task to balance the opposing interests, but it is not an impossible one either. . . . Success lies in providing a workable formula which encompasses, balances, and protects all interests, yet places emphasis on the fullest responsible disclosure."[23] In discussing exemption (b)(6), the House Committee report goes on to say: "The limitation of a 'clearly unwarranted invasion of personal privacy' provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to government information by excluding those kinds of files the disclosure of which might harm the individual."[24]

This approach was praised by some for recognizing a right of privacy and providing for it at a time when few were concerned about informational privacy. At the same time, it has been criticized for requiring disclosure under circumstances that would be an "unwarranted invasion of personal privacy" but not "clearly" so. For others, there seemed to be an inconsistency between the notion of a "right of privacy" and the notion of a "warranted" invasion of that privacy.

Privacy concerns have been argued in the courts under both the b4[25] and b6[26] exemptions. The argument under the b4 exemption has centered on "privileged or confidential." Many have argued that this should include material given to the government under a good faith understanding of confidentiality. Prof. Davis has said, "Obviously, the good faith understanding that the information will be kept confidential should be honored. But the statutory words clearly limit the exemption to 'commercial or financial information.'"[27] While the *Attorney General's Memorandum*[28] and the legislative history both indicate a broader reading of b4, the courts have followed the fairly clear literal meaning of the statute.[29] Even when the material is commercial or financial, a promise of confidentiality is not

---

[23]SENATE COMM. ON THE JUDICIARY, CLARIFYING AND PROTECTING THE RIGHT OF THE PUBLIC TO INFORMATION, AND FOR OTHER PURPOSES, S. REP. No. 813, 89th Cong., 1st Sess. 3 (1965).

[24]*Supra* note 22.

[25]b4 Trade secrets and commercial or financial information obtained from a person and privileged or confidential.

[26]b6 Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

[27]Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761, 787 (1967).

[28]20 AD. LAW REV. 263, 300 (1968).

[29]Consumer Union of United States, Inc. v. Veterans Administration, 301 F. Supp. 796 (S.D.N.Y. 1969), *appeal dismissed as moot*, 436 F.2d 1363 (1971).

enough to sustain exemption.[30] "To summarize, commercial or financial matter is 'confidential' for purposes of the exemption if disclosure of the information is likely to have either of the following effects: 1) to impair the government's ability to obtain necessary information in the future; or 2) to cause substantial harm to the competitive position of the person from whom the information was obtained."[31] Exemption b4 has been found to apply to individual, personal financial information as distinguished from corporate or business information but only within the narrow confines of the court's interpretation of b4.[32]

Most FOIA cases argued on privacy grounds are argued under the b6 exemption. The courts have had difficulty with "clearly unwarranted invasion of privacy." The approach now followed by the D.C. Circuit, the Second Circuit,[33] and the Third Circuit[34] is the balancing test originally put forth in *Getman v. National Labor Relations Board*.[35] In that decision Judge Skelly Wright said, "Exemption 6 requires a court reviewing the matter *de novo* to balance the right of privacy of affected individuals against the right of the public to be informed; and the statutory language 'clearly unwarranted' instructs the court to tilt the balance in favor of disclosure."[36] In *Wine Hobby U.S.A. v. United States Internal Revenue Service* the Third Circuit noted that the balancing done by the Getman court refers only to the b6 exemption. "Only non-exempt material is available to 'any person.' There is nothing that precludes balancing to determine whether particular information is within a statutory exemption."[37]

As this test has been applied by the courts that have followed the D.C. Circuit, there have been two considerations: 1) whether there is an invasion of privacy; and 2) whether that invasion is "warranted" by the use the requestor of the information is going to make of it. In *Getman* the release of the names and addresses of employees was found to invade the privacy of the employees, but the significant nature of the research project involved "warranted" that minor invasion. There have been two other cases involving the release of names and addresses. In *Ditlow v. Schultz*[38] the court found the use unwarranted because it was not clear that the

---

[30]Sears, Roebuck and Co. v. GSA, 384 F. Supp. 996 (D.D.C. 1974); Petkas v. Staats, 501 F.2d 887, (D.C. Cir. 1974).

[31]National Parks and Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974).

[32]Rural Housing Alliance v. U.S. Dept. of Agr., 498 F.2d 73 (D.C. Cir. 1974); Ditlow v. Schultz, 379 F. Supp. 326 (D.D.C. 1974).

[33]Rose v. Department of the Air Force, 495 F.2d 261 (1974).

[34]Wine Hobby U.S.A., Inc. v. United States Internal Rev. Serv., 502 F.2d 133 (1974).

[35]450 F.2d 670 (D.C. Cir. 1971), *app'l for stay or order denied*. 404 U.S. 1204 (1971).

[36]*Id*

[37]*Supra* note 34.

[38]379 F. Supp. 326 (D.D.C. 1974).

requestor would be able to maintain the class action suit for which he sought the names; and, if he could maintain the suit, the names would be available through another source (*i.e.*, through discovery). In *Wine Hobby* the court found the proposed use did not warrant disclosure because the use was "commercial exploitation (which is) wholly unrelated to the purposes of FOIA."[39]

The degree of the invasion of privacy was far more serious in two other b6 cases. In Rural Housing Alliance v. United States Department of Agriculture,[40] the information sought was "detailed and intimate case histories of specified named individuals." In *Rose v. Department of the Air Force*,[41] the material sought was case summaries of Honor and Ethic's Code adjudications at the Air Force Academy. In both cases it was argued strenuously that there was no way to delete identifying material sufficiently to protect the privacy of reported individuals. In both cases, the court remanded with instructions to attempt to delete identifying details.

In *Robles v. Environmental Protection Agency* the Fourth Circuit did not consider the proposed use of the requested material and expressly disavowed balancing. "As Professor Davis has so convincingly emphasized, the earlier provision in the Administrative Procedure Act 'provided for disclosure to persons properly and directly concerned.' That was changed to 'any person', demonstrating beyond argument that disclosure was never to 'depend upon the interest or lack of interest of the party seeking disclosure.'"[42] While the court found there were significant privacy questions, the court concluded that they did not reach "clearly unwarranted" proportions. Most significant to this court was that no householder had objected to the disclosure.

THE ABSOLUTE TEST FOR PRIVACY

One way to assure privacy within the FOIA is to determine what materials should be protected from disclosure for privacy reasons, designate them clearly, and exempt them from disclosure by statute. Such material would be protected from disclosure under FOIA by the b3 exemption "specifically exempted from disclosure by statute." This approach fits with the general

---

[39] *Supra* note 34.

[40] 498 F.2d 73 (D.C. Cir. 1974).

[41] 495 F.2d 261 (2nd Cir. 1974).

[42] 484 F.2d 843, 847 (1973); *see also* Note, *Invasion of Privacy and the Freedom of Information Act: Getman v. NLRB*, 40 G.W.L. Rev. 527 (1972), for a critical review of the balancing test used by the Getman court.

approach that Congress, not the agencies or the courts, should make the decisions on how to balance the interests between disclosure and the privacy concerns of individuals and the government. Congress rejected the equitable tests of the prior Public Information section of the Administrative Procedure Act[43] for a policy that requires release of requested material except for material specifically exempted from disclosure. Congress weighed the interests involved and determined which materials to exempt from the disclosure requirement originally and can, in its concern for individual privacy, specifically exempt more material.

If Congress by statute were to exempt certain material from disclosure, the court's only function in ruling on a challenge to order disclosure would be to determine that such a statute did exist and that the material sought fell within the statute. This approach has been called the per se approach because the court does not consider the merits of disclosure or exemption.[44]

The primary advantage of this approach is its ease of implementation. Agency personnel should be able to understand what material is included and, therefore, what material is to be disclosed. The recent FOIA amendments are primarily directed toward more prompt agency compliance; if this goal is to be achieved, the clearest possible standards must be given. Currently, interpretation of the court-made standards as to privacy and the FOIA require agency attention at the highest level and, generally, referral to the Justice Department Committee of FOIA for a legal opinion, obviously a time-consuming process.[45]

The other major advantage of the absolute test is that it assures the confidentiality of particular data. The President's Commission on Federal Statistics concluded: "The only way to assure the confidentiality of particular data is by a statute requiring that those data be held in confidence. In such a case, the statute requires the agency to resist a request for the data, and it can justify its refusal in a suit brought under the Act on the grounds of the third exemption."[46] Any test which balances interests might not succeed in guaranteeing the confidentiality of any particular data.

The difficulty with this method is specifying what material should be exempted. As has been noted before, there is no clear definition of what is private information deserving confidential treatment. One method to accommodate the needs of confidentiality on a case-by-case basis is to give

---

[43]Sec. 3 ADMINISTRATIVE PROCEDURE ACT *as amended by* Pub. L. 89-481.

[44]Note, *The FOIA's Investigatory File Exemption*, 42 G.W.L. REV. 87 (1974).

[45]Saloschin, *Administering the FOIA: An Insider's View*, in GOVERNMENT SECRECY IN AMERICA: NONE OF YOUR BUSINESS 192 (1974).

[46]1 PRESIDENT'S COMMISSION ON FEDERAL STATISTICS, FEDERAL STATISTICS 209 (1971).

agency heads the authority to declare certain material confidential. A variation on this method is to provide an exemption if agencies have promised confidential treatment at the time of collection of the information. This method has the obvious problem that it gives to agencies the very discretion with regard to disclosure that the FOIA attempts to remove from agencies. The courts have generally been unwilling to accept such agency determinations as not providing a sufficiently specific exemption as required by b3.[47]

Another case-by-case approach is where Congress excludes specific material from disclosure by statute. The Census Law, for example, exempts all material furnished under the provisions of the Act from any type of disclosure by which any particular establishment or individual can be identified.[48] In addition the Census Law limits the use of the material to statistical purposes and further limits who may examine the individual reports.[49] The problem with this approach is that Congress would have to identify each of those federal programs which require such an exemption from FOIA disclosure, a possible unworkable prospect.

An example of an effort to take a broader, more inclusive approach to the problem was that taken by the Moorhead Bill.[50] While the Moorhead Bill, as here analyzed, was not enacted into law, an analysis of it is helpful to an understanding of the way in which an absolute test for privacy would relate to FOIA.[51] The Moorhead Bill used an absolute test for privacy by specifically exempting from disclosure by statute (under (b)(3)) all personally identifiable material contained in record systems. The proposed act "permits an individual to prevent records pertaining to him obtained by the agencies for a particular purpose from being used or made available for another purpose without his consent."[52] This obviously conflicted with FOIA access and yet there seems to be only slight recognition of this conflict. There is one reference in the Committee Report to the FOIA disclosure requirements. "H.R. 16373 would make all individually identifiable information in government files exempt from public disclosure."[53] The

---

[47]Cutler v. Civil Aeronautics Bd., 375 F. Supp. 722 (D.D.C. 1974); Stretch v. Weinberger, 495 F.2d 639, (3rd Cir. 1974). Bristol-Myers Company v. Federal Trade Commission, 424 F.2d 935 (D.C. Cir. 1970), *cert. den.* 400 U.S. 824 (1970); Consumers Union of United States, Inc. v. Veterans Administration, 301 F. Supp. 796 (S.D.N.Y. 1969) *app. dism. as moot,* 436 F.2d 1363 (1971).

[48]Census Law 13 U.S.C. 9(a)(2)(1954).

[49]*Id.* 13 U.S.C. 9(a)(1) and (3)(1954).

[50]H.R. 16373.

[51]All references are to the Moorhead Bill H.R. 16373 as it appeared on Nov. 21, 1974, when it was discussed, amended, and passed by the House (120 Cong. Rec. No. 163 H 10950-71).

[52]H.R. 16373—proposed 552a(a)(4).

[53]H.R. Rep. No. 93-1416, 93rd Cong., 2nd Sess. 4 (1974).

report goes on to say that "The Committee does not desire that agencies cease making individually identifiable records open to the public, including the press, for inspection and copying. On the contrary it believes the public interest requires the disclosure of some personal information. . . . The Committee merely intends that agencies consider the disclosure of this type of information on a category-by-category basis and allow by published rule only those disclosures which would not violate the spirit of the FOIA by constituting 'clearly unwarranted invasions of personal privacy.'" This last reference is to the "routine use" provision of the bill which required the agencies to publish in the *Federal Register* all of the uses to which their records will be put in the normal course of business.[54] Transfer of the record for any purpose not so indicated would require the written consent of the individual to whom the record pertained.

While it seems clear that any personally identifiable material would have been exempt from mandatory disclosure, the Committee Report indicates their desire for voluntary disclosure. However, the mechanism provided for voluntary disclosure seems ill suited to that end. The publication in the *Federal Register* of permitted disclosures which would not violate the spirit of the FOIA by constituting "clearly unwarranted invasions of personal privacy" is not compatible with the definition used of that phrase by most courts. As has been noted, most courts have followed the D.C. Circuit test in *Getman v. National Labor Relations Board*[55] which involves balancing the interests of the requestor of the information with the interest in protecting individual privacy. When the agency publishes an intent to release material pursuant to FOIA requests as a "routine use" they do not know who will request the material and what use will be made of the material.

H.R. 16373 did permit the release of individually identifiable material contained in a system of records with the prior written consent of the individual to whom the record pertains. While the mechanism for obtaining this written consent was not specified, it presumably could be arranged. But, there may well be situations where the public right to know should supercede the individual's unwillingness to give consent. The most obvious situation is where the government's treatment of an individual or a group of individuals has been inappropriate but favorable to those individuals. It is not realistic to rely on those favored individuals to give consent to the disclosure.

An absolute test for privacy, such as that used by the Moorhead Bill, protects privacy at the expense of FOIA access. The significant advantage

---

[54] H.R. 16373 3(2)(D).

[55] 450 F.2d 670 (D.C. Cir. 1971) *app'l for stay or order denied*. 404 U.S. 1204 (1971).

of the approach is its ease of application. The decision to err on the side of privacy and confidentiality is entirely consistent with a basic constitutional right of privacy. The obvious disadvantage is that it prohibits the disclosure of any material within the classification, even material not necessarily private. Such prohibition of disclosure in this area is inconsistent with the right to know.

THE RELATIVE TEST FOR PRIVACY —

The Privacy Act of 1974

Another method to reconcile the conflict between the desire to provide access to government information and the desire to keep confidential personal information in government files is to provide, by statute, a balancing test between these two interests. This approach recognizes what Professor Davis has described as "[T]he customary practice of normal people, who often disclose to those who have a special reason for knowing and withhold from those who do not. Private practices frequently depend on the difference between disclosure to the public and disclosure to one person or a restricted few."[56] Providing such a test requires defining the interests to be considered and the weight to be given to these factors. In order for such a balancing test to be functional it would be necessary to provide direction in cases where the interests are relatively equal, whether to err on the side of access to information or on the side of confidentiality. As seen before most courts currently apply the FOIA (b)(6) exemption as a balancing test, but a clearer test would enlarge (b)(6) to include all invasions of privacy, not just those related to "personnel and medical files and similar files." Also a test must clarify for the agencies and courts the congressional intent of the use of the expression "clearly unwarranted invasion of personal privacy." Finally, it would be necessary to require that information the disclosure of which would constitute an invasion of privacy is not only exempt but is prohibited from disclosure.

The FOIA itself has been used in a few cases to prohibit disclosure. In these 'reverse' FOIA cases an action is brought by the party seeking to prohibit disclosure. While at first the courts were hesitant to find jurisdiction under FOIA to prohibit disclosure,[57] in more recent cases the courts have found jurisdiction to prohibit disclosure of information which

---

[56]Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761, 765 (1967).

[57]Charles River Park "A" Inc. v. Dept. of Housing and Urban Development, 360 F. Supp. 212 (D.D.C. 1973); Sears Roebuck & Co. v. G.S.A., 384 F. Supp. 996 (1974)

fell within the (b)(4) and (b)(6) exemptions.[58] While the result of these decisions is probably appropriate, the reasoning is strained. Under no circumstances does the FOIA itself, as written, deny access. It merely defines the circumstances under which agencies are permitted to refuse access. Some of the interests protected by these exemptions, such as personal privacy, are significant enough to warrant the further protection of a mechanism for prohibiting disclosure.

An interesting approach to providing a balancing test which does prohibit disclosure was that taken by the Ervin Bill and adopted by the Privacy Act. The Privacy Act exempts from the nondisclosure provisions of the Act those disclosures required under FOIA.[59] The result of this is a balancing test to see if material is required to be released; for, as seen before, most circuits are now following the balancing or relative test developed in *Getman*.[60] If the material is not required to be released by FOIA, it is prohibited from release by the Privacy Act unless it satisfies another exemption of the Act.

The Privacy Act of 1974[61] has four main requirements for federal agencies: limit the collection and maintenance of data; index and publish a guide to all record systems; grant access to record systems; and limit disclosure of information in a record system. The Act is the product of a last-minute compromise between the House and Senate which did not go through the normal conference committee procedure. Rather, the compromise was worked out between the two committee staffs and the principal sponsors in the House and Senate. For this reason there is not a conference committee report on the Act, but rather a document which was introduced into the record at the time the compromise bill was offered as an amendment to the pending privacy bills before the House[62] and Senate.[63]

The most effective portion of the Privacy Act is probably the requirement to publish annually a description of each system of records.[64] There is no exemption to this requirement based on the idea that there should be no system of records whose very existence is secret. While the index itself will no doubt be ponderous and of primary interest to the student of government, it is widely felt that this requirement, along with the access

---

[58]McCoy v. Weinberger, 386 F. Supp. 504 (1974); Neal-Cooper Grain Co. v. Kissinger, 385 F. Supp. 769 (1974); Hughes Aircraft Co. v. Schlesinger, 384 F. Supp. 292 (1974).

[59]5 U.S.C. 552a(b)(2).

[60]Getman v. National Labor Relations Board, 450 F.2d 670 (D.C.C. 1971), *app'l for stay of order denied*, 404 U.S. 1204 (1971).

[61]Pub. L. 93-599, 552a.

[62]120 CONG. REC. H. 12243 (daily ed. Dec. 18, 1974).

[63]120 CONG. REC. S. 21815 (daily ed. Dec. 17, 1974).

[64]Pub. L. 93-599, 552a (e)(4).

requirements, may cause government agencies to evaluate their information needs and eliminate and consolidate many existing systems of records.

The Privacy Act limits the government's ability to collect information by requiring no record describing how any individual exercises his First Amendment rights unless expressly authorized by statute or by the individual about whom the record is maintained or pertinent to an authorized law enforcement activity.[65] The Act also requires that agencies maintain only such information about an individual as is necessary to accomplish a purpose that the agency is required to accomplish by statute or executive order of the President.[66] The enforcement procedures for existing systems are weak but new record systems must be reported to the Office of Management and Budget and the Congress prior to implementation.[67]

The Act requires that agencies establish procedures to give an individual access to records about himself and to allow him to challenge the information. Exemptions can be invoked for the records of the CIA, criminal law enforcement agencies, classified material, investigatory files for law enforcement purposes, protective service records, statistical records, and investigatory files for federal employment or military service or promotion but only to the extent necessary to prevent revealing a confidential source.[68] In addition to these exemptions this requirement does not fulfill the need of an individual to know what material about him is in government files because only information in a system of records is covered and only if that information is retrieved by reference to the named individual. If information about someone appears in any other file such as one about a different person or a business file, the person would not have access to it under the Privacy Act.

The Act also limits the disclosure of information in a system of records and requires an accounting of most disclosures. This is probably the weakest provision because of the number of exemptions. Disclosure of information in a system of records without the consent of the individual is not permitted unless one of the exemptions are met. The first exemption is for disclosure within the agency to those officers and employees of the agency who have a need for the record in the performance of their duties.[69] The key to this provision is the definition of agency; the smaller the subunit, obviously, the more limited the disclosure possibilities. The definition of

---

[65] *Id.* (e)(7).
[66] *Id.* (e)(1).
[67] *Id.* (o).
[68] *Id.* (j) and (k) (1-7).
[69] *Id.* (b)(1).

agency is the same as the FOIA. There is a suggestion in a letter from the Assistant Attorney General that the definitions of agency may be different for different portions of the Act.[70]

Disclosure is permitted for a routine use[71] defined as a use of a record for a purpose which is compatible with the purpose for which it was collected,[72] if that routine use has been identified in the annual public notice.[73] Disclosure is also permitted for release to the Bureau of the Census, for statistical and research purposes, to the National Archieves, for law enforcement purposes, under emergency circumstances, to Congress and any Congressional Committee, to the General Accounting Office, pursuant to a court order and if required by FOIA.[74]

With reference to the disclosure exemption for FOIA, the report says "Perhaps the most difficult task in drafting federal privacy legislation was that of determining the proper balance between the public's right to know about the conduct of their government and their equally important right to have information which is personal to them maintained with the greatest degree of confidence by federal agencies. . . .This compromise is designed to preserve the status quo as interpreted by the courts regarding the disclosure of personal information under that section."[75]

While the committee report suggests that this provision maintains the status quo, it clearly does not. The FOIA taken alone requires disclosure unless it would be a "clearly unwarranted invasion of personal privacy" and, even then, disclosure is allowed. The general tenor of FOIA is always to err on the side of disclosure, to encourage disclosure in the close case. However, the Privacy Act only permits disclosure when it is *required* by the FOIA. The status quo would have been maintained by the provisions of the original Ervin Bill, which simply exempted from the requirements of the privacy bill material required or *permitted* to be released under the FOIA.[76] Without the additional word "permitted," the grey area has been removed and in its place is an absolute line; disclosure is either required by the FOIA or forbidden by the Privacy Act.

The Act does not indicate which side to favor in the close case, and both the Act and the FOIA provide for civil and criminal penalties if agencies don't comply. The Privacy Act does require a "willful or intentional"[77]

---

[70]Letter from Antonin Scalia, Office of Legal Counsel, Department of Justice to James T. Lynn, Director, Office of Management and Budget, April 14, 1975.

[71]Pub. L. 93-599, 552a(b)(3).

[72]*Id.* (a)(7).

[73]*Id.* (e)(11).

[74]*Id.* (b) (4-11) (b)(2).

[75]120 CONG. REC. S. 21816 (daily ed. Dec. 17, 1974).

[76]S. 3418 202(c).

[77]552a(g)(4).

failure on the part of the agency to comply with the Act, to impose civil or criminal liabilities; under circumstances of a direct conflict between the two Acts, it seems unlikely a court would find that standard met. If the court did not agree that the case was close, the court could impose court costs including attorneys' fees on the agency, and civil costs for damages sustained.

Not all cases under (b)(6) of the FOIA will be covered by the Privacy Act; and, to that material not covered by the Act, the status quo will be maintained. The definitions of the Act are important to FOIA not only because they define how much of the (b)(6) exemption is covered by the Privacy Act but because they also are an indication of the congressional limits of privacy. The Privacy Act refers to "records" and "system of records." "[T]he term record means any item, collection or grouping of information about an individual that is maintained by an agency, including but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph."[78] "The staff compromise defines records as including not only collections of information about individuals but also an 'item' of information about an individual."[79] "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying member, symbol, or other identifying particular assigned to the individual."[80] There has been some debate as to whether this means "actually is retrieved by identifier" or "can be retrieved by identifier." While it would seem that Congress clearly intended to use 'is retrieved' and not 'can be retrieved,' it seems an unnecessarily difficult test. Does "is retrieved" mean that it was once so retrieved; what if that once was this week, three weeks ago, three years ago?

Even when material is within the material covered by the Privacy Act, and it is not required to be disclosed under FOIA, it might still not be prohibited from disclosure by the Privacy Act. Under the Act material can be disclosed either with the prior written consent of the subject[81] or if the agency makes disclosure pursuant to a FOIA request for a "routine use"[82] of the material. It seems unlikely that agencies would make such disclosure a 'routine use' but if they did, the Privacy Act would not prohibit disclosures under FOIA

---

[78] 552a(a)(4).
[79] 120 Cong. Rec. S. 21822 (daily ed. Dec. 17, 1974).
[80] 552a(a)(5).
[81] 552a(b).
[82] 552a(b)(3).

of even those disclosures which would be a "clearly unwarranted invasion of personal privacy."

The Act provides that if an agency is required to provide personal information about an individual pursuant to compulsory legal process, the agency shall make reasonable efforts to serve advance notice on the individual before it makes available the information.[83] The Senate Committee Report notes that the purpose of this section is to allow the individual advance notice so that he may take appropriate legal steps to suppress the subpoena and also to assure that the individual will be able to exercise rights under this Act to check the data for accuracy.[84] The only way to reconcile the lack of requiring such notice for FOIA disclosures is to assume that the FOIA itself protects personal privacy while compulsory legal process has no such requirement. It would seem appropriate for agencies and courts to use the example of the latter provision to require advance notice in some instances of disclosure under FOIA even though the Act excludes FOIA from such a requirement. It would not be appropriate in cases where there were very large numbers of data subjects and the privacy concern was minimal, but it might well be appropriate in cases where the privacy concern was very great and the number of individuals involved not prohibitive.[85]

The Act prohibits the renting or selling of mailing lists unless specifically authorized by law. "This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public."[86] "In other words, such lists can not be withheld by an agency, unless it determines that the release would constitute 'a clearly unwarranted invasion of privacy'. . . . Thus, the language of the bill before us does not ban the release of such lists where either sale or rental is not involved. . . . This measure now before us would preserve the current practices and interpretations of this part of the FOIA (by the federal courts) as they deal with federal agency mailing lists."[87] The principle case dealing with the release of mailing lists in a commercial setting is a Third Circuit case. The court there found that such a request was an unwarranted invasion of privacy since "commercial exploitation is wholly unrelated to the purposes of FOIA."[88]

---

[83] 552a(e)(8).

[84] S. Rep. No. 93-1183, 93rd Cong., 2d Sess. 66-67 (1974).

[85] See Robles v. Environmental Protection Agency, 484 F.2d 843 (4th Cir. 1973); Rural Housing Alliance v. United States Dept. of Agr., 498 F.2d 73 (D.C. Cir. 1974); Rose v. Dept. of Air Force, 495 F.2d 261 (2d Cir. 1974) for examples of cases where it might be appropriate.

[86] 552a(n).

[87] 120 Cong. Rec. H. 12246 (daily ed. Dec. 18, 1974). (Remarks of Congressman Moorhead).

[88] Wine Hobby U.S.A., Inc. v. Internal Revenue Serv., 502 F.2d 133 (1974).

The Privacy Act provides for the public interest in disclosure of certain personal information. Under the FOIA if the public need for the information is demonstrated, then the invasion of personal privacy caused by the disclosure of personal information may be warranted. Under this procedure a very strong showing of public need may justify a very large invasion of privacy. The fear that the FOIA does not sufficiently protect personal privacy was expressed by President Ford when he signed the Privacy Act. "I am disappointed that the provisions for disclosure of personal information by agencies make no substantive change in the current law. The latter in my opinion does not adequately protect the individual against unnecessary disclosures of personal information."[89]

In addition to this fear the most serious defect of the approach of the Privacy Act is that it would appear to subject almost all requests for disclosure of personal information to court test. Even if the original statutory language of "permitted disclosures" had remained, agency personnel would have a difficult task to apply the balancing test; what constitutes a "warranted" invasion of privacy is not clear. The only ones able to achieve access to material in this area will be those with the time and the money to pursue the necessary court challenge. Generally, the circuit courts have required an indexing of all the material involved in the controversy, an itemized justification for refusal to disclose keyed to the index, and *in camera* inspection of the material by the court to determine if the refusal was justified. The District Court for the District of Columbia, on the remand of *Vaughn v. Rosen*,[90] developed a record to indicate just how time consuming this requirement can be. The material involved in that case would have filled 17 standard-sized five-drawer filing cabinets and the time to index the material would take 10,257.1 man hours or 4.93 man years at a total cost of $96,176.00. In that case the court, instead, used nine representative samples with the consent of all parties.

For a balancing or relative test to be workable, Congress will have to make more decisions than they did in the Privacy Act. The first must be whether the Congress wants to make the courts an instrument for the implementation of the Act or whether a means for implementing the Act outside the court is to be developed. The second is the really hard question of the close case, should the agencies err on the side of disclosure or non-disclosure? Hopefully Congress could also address more clearly just what type of material is to be protected. Perhaps the Privacy Study Commission,[91] established by the Act, will help define the terms more

[89] 11 Weekly Compilation of Presidential Documents 7, (No. 1, Jan. 1, 1975).

[90] 383 F. Supp. 1049 (1974) on remand from 484 F.2d 820 (D.D.C. 1973), *cert. denied*, 415 U.S. 977 (1974).

[91] 552a 5(a)(1).

clearly. Even with a congressional approach that attempted to deal with these issues, a balancing test would still be a difficult standard to apply because it is a relative standard of elements not easily defined.

DELETION OF IDENTIFIABLE MATERIAL

One of the most obvious ways to reconcile the conflict between access and privacy in a number of cases is to provide a mechanism for deleting identifiable material and providing a means for the release of segregable portions of files. The FOIA provides that "To the extent necessary to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction."[92] In the interest of privacy a further refinement might require that whenever the material involves any personally identifiable material that the identifiable material be deleted whenever the requestor's purpose can be served by deleted form. Even this use of deletion has the problem of raising suspicions on the part of the information recipients that more than just identifying details were deleted. To protect against this and other possible abuses of the deletion tool, courts have ordered that all proposed deletions be submitted to the court for *in camera* inspection, obviously a very time-consuming process for the courts and the agencies.

The two most significant criticisms of deletions is that it may not succeed in protecting the privacy of the individual involved[93] and that it makes compliance with FOIA much more complicated, therefore more expensive and more time consuming. Congress has made clear its intent to require the release of any reasonable segregable portion of a record after the deletion of portions which may be exempted by the addition of this specific requirement in the 1974 amendments. Deletions and segregation make compliance more difficult, requiring attention from higher level personnel, and therefore make general access much slower and more expensive. However, without deletions there would not be any access to this body of information, or it would be released with the concommitant invasion of privacy.

It is not clear whether the Privacy Act allows for deletions as a way of reconciling these interests. It permits the release of material in a non-identifiable form if it will be used solely as a statistical research or reporting record.[94] This appears to be the only release specifically permitted for

[92] 5 U.S.C. 552 (a)(2).
[93] *Infra* at notes 45, 54.
[94] 552a(b)(5).

material to be disclosed in a non-identifiable form. No committee report makes clear whether the intent was to limit release of non-identifiable material only to statistical and research use or to limit disclosures for statistical and research use only to non-identifiable information. For FOIA purposes the question is a definitional one: does a record under the Privacy Act cease being such when it is reassembled in its deleted or scrubbed form? Logic should compel the result that it is no longer a record under the Act even if the reassembled record was made only to fulfill an FOIA request. The only reason for not permitting releases of material in non-identifiable form out of concern for the right of privacy is the conclusion that it cannot be done without some fear that the individual's privacy will still be compromised; in other words, that the non-identifiable form is still identifiable. While this may be true in some limited cases, in the vast majority it would not seem to be a serious concern.[95]

THE TASK FOR CONGRESS

The FOIA has been frequently criticized for imprecise draftsmanship—most recently by Judge Gesell. "Accordingly, as is usually the case where the court must attempt to apply this imprecise and poorly drafted statute to a situation apparently never contemplated by the Congress, it becomes necessary to resolve the controversy by reliance on the high gloss which the learned decisions of this circuit have been required to place on the legislation."[96] Privacy legislation could have assisted the agencies and the courts in the application of the (b)(6) exemption of the FOIA but the Privacy Act of 1974 fails to address the issues. Unless there is a clear recognition of the relationship between the right of privacy and the right to know neither will be well served.

There is a general recognition that the Privacy Act of 1974 is a first effort and a great hope that experience with this legislation will help clarify these issues and improve future attempts to refine this legislation. It must be hoped that Congress will soon recognize their responsibility to legislate more clearly the relationship between the right of privacy and the right of access. The current Privacy Act succeeds only in drawing a line and requiring disclosure on one side of the line and forbidding it on the other.

But the difficult question of where that line should be drawn, of what factors should be considered, of what weight should be given to the considerations of privacy and access have been left to the agencies and

[95] Legal Aid Society of Alameda County v. Schultz, 349 F. Supp. 771 (N.D. Cal. 1972).

[96] Washington Research Proj., Inc. v. Dept. of H.E.W., 366 F. Supp. 929 (D.D.C. 1973), *rev'd in part on other grounds*, 504 F.2d 238 (D.C. Cir. 1974).

ultimately the courts. Congress chose a relative test for the relationship between the right of privacy and the right of access. While a relative test is more reflective of the elements of privacy, an absolute test, such as that proposed by the Moorhead Bill, may be a practical necessity. It would take an incredible degree of refinement to fashion a relative test that could be implemented readily by agency personnel. An absolute test with clearly defined terms could be implemented.

There is not one correct way of relating and reconciling the two; rather there is a range of choices to be made. An absolute privilege from disclosure for all personal information has a major advantage in its ease of administration and the virtue of clearly protecting privacy. A balancing test recognizes the demands of both and provides for the maximum access compatible with protecting privacy. It has the advantage of recognizing the citizen's need to know the information upon which the government is making decisions.

Both the Privacy Act of 1974 and the FOIA are important pieces of legislation that need to work and need workable definitions so that they can be implemented outside of the courtroom. If the legislators do not make these decisions, the courts will be forced to. This has the double disadvantage of turning judges into legislators and making the courts an agency for the implementation of the Privacy Act and the FOIA. This is not a workable method for the implementation of either of these Acts. Both the right of privacy and the right to know are important values; but legislation in this area must recognize the two together, where they are compatible and where they conflict.

[From the Wall Street Journal, Nov. 13, 1974]

The Continuing Problem of Privacy

(By Arlen J. Large)

Washington—Barry Goldwater Jr., a California Congressman and the Senator's son, boasts that the almost-ended 93rd Congress will be known as "The Privacy Congress."

All year, members of Congress have been making speeches and holding hearings on the virtues of curbing the computerized snoopers of big government and big business. "A society numbered, punched and filed by government cannot be free," is one of the snappy 1974 sayings of Sen. Sam Ervin.

Complaints about a numbered society focus on the ubiquitous Social Security number, which is being used increasingly as a "universal identifier" in business and government, including state and local government. When your number gets into computers used variously for phone-company billing, drivers licenses, voting rosters, income-tax records and bank accounts there'll be no place to hide.

So one of the privacy-protection bills introduced earlier this year provided that unless some federal law requires it, as with an income-tax return, nobody could make you give out your Social Security number at all.

There's a good chance that a privacy-protection bill will be enacted by Congress during the lame-duck session this year. But it won't include any restriction on current government or business use of Social Security numbers in data banks. The Senate committee considering the bill had second thoughts and took out the provision after being told it would have a devastating effect on data-bank costs throughout the economy.

The backdown on Social Security numbers shows how hard it is for "The Privacy Congress" to go much beyond speechmaking on the evils of data banks that know too much about everybody. The federal bureaucracy would be at least potentially affected by the pending privacy bill, but it naturally doesn't want to be inconvenienced and is resisting the legislation. Sen. Ervin recalls that when he tried to make an inventory of data banks in federal agencies, he met "evasion, delay, inadequate and cavalier responses, and all too often a laziness born of a resentment that anyone should be inquiring about their activities."

But in many cases federal agencies ask people all those nosy questions to carry out laws passed by Congress itself. In a recent discussion of privacy problems Associate Supreme Court Justice William Rehnquist observed that when Congress sets up, say, a student loan program, the government automatically wants more dope on the student. Justice Rehnquist continued:

"I think few would disagree with the proposition that the government is present in the lives of all of us today in a way that would have been inconceivable even 50 years ago. From this there flows at least a rebuttable presumption that the government will know more about each of us than it did 50 years ago, and that in a very real sense we will have that much less privacy."

When Congress Acts

When Congress tries to solve a problem, it sometimes authorizes giant invasions of privacy as a consequence. In 1970, in pursuit of big-time swindlers and tax cheats, it gave Treasury agents authority to trace checks drawn on personal bank accounts and to otherwise run barefoot through a person's financial records. And deciding that secret political fund-raising is bad, Congress in 1971 required public disclosure of the name of everyone who gives a federal candidate more than $100. That has had some very salutary effects on the behavior of politicians and donors alike, but some legal experts think the invasion of privacy is so gross as to be unconstitutional.

Moreover, Congress seems no more willing than the bureaucracy to inconvenience itself on privacy matters. Among other things, the pending privacy bill is intended to make it easier for someone to find out if he's mentioned in a federal file or data bank somewhere, to inspect what it says about him and to make corrections. The idea is borrowed from a 1970 law giving people access to their own files kept by private credit-reporting companies. The perfectly sensible point is to keep errors in someone's file from swirling through computer after computer in government and business, making that person's Social Security number a red flag of misery.

Some of the juiciest files the government maintains on people are kept by the House Internal Security Committee, which tries to monitor persons with suspicious politics. Someone who thinks his name is in that file might understandably be curious about what it says, and whether it's the truth. But if he asks the committee to see his file he's turned away, unless he can get the information through his own Congressman. The new privacy bill wouldn't change that. Congress doesn't like pests.

Executive Branch resistance to privacy legislation doesn't have to be very strong for the lawmakers to cave in. Sen. Ervin has been pushing a statutory ban on the kind of Army spying on civilians that occurred during the 1960s, but the Army says the bill isn't needed because the spying has stopped. The bill is dead. Another Ervin bill would forbid the Civil Service Commission to ask federal job applicants impertinent questions about their sex lives and religious beliefs; the bill has repeatedly passed the Senate, but Civil Service officials always persuade the House to kill it.

The Justice Department itself has proposed legislative restrictions on the way old arrest and conviction records can be taken from federal-state data banks on criminals and passed around to employers and banks. But there's disagreement in the department over the bill's details. The FBI doesn't like the idea of keeping old criminal records from police officers, and news organizations worry that reporters might be denied access to court records. With all that trouble, the bill is bogged down.

Yet the atmosphere is ripe for some kind of action on legislation with a "privacy" label, and the catalyst, of course, is Watergate. What the Nixon White House did to the privacy of a California psychiatrist, and others, was already against the law, but it raised such a stark spectre of Big Brother government that more law is felt necessary. "In a certain way, I suppose that Richard Nixon may go down in history as the patron saint of privacy legislation," said Alan Westin, a Columbia University professor of government, in testimony before a Senate committee this year.

Both the House and Senate Government Operations Committees have drafted companion privacy bills that are similar, and floor action is scheduled in both houses after the current election recess. More legislating is required to produce a final product, but its main points look fairly clear.

The final bill undoubtedly will require every federal agency that keeps files or computerized data on citizens to confess it publicly, and to explain what the information is for. This would carry out a dictum of President Ford, who's shown enthusiasm for the privacy-protection effort, that "the federal government should not maintain any record-keeping system whose very existence is secret from either the elected representatives of the people or the public at large."

Congress earlier this year was startled to learn that plans were afoot to link the computers of several departments into a scary new system called Fednet. Portests from Congressmen and others, including Mr. Ford, then-Vice President, caused this plan to be shelved.

The bill also would let an individual inspect an agency's records about him and make corrections, but there are important exceptions. An investigatory file is apt to be what a person most wants to see, but that would be kept shut, as would files dealing with defense and foreign policy. And drafters excluded corporations, fearing big companies would be forever getting into fights with the Justice Department over material accumulated in files for potential antitrust cases.

FIRST AMENDMENT GUIDELINES

The final bill probably will set out new guidelines for federal agencies that poke into First Amendment areas, asking questions about religion or politics but those questions won't be banned entirely. And agencies will face new restrictions on transferring among themselves data-bank information about citizens. In some cases, such as when the Small Business Administration wants to see a credit rating kept on a loan applicant by the Federal Housing Administration, the applicant could deny permission for the data transfer.

The Senate committee's version of the bill also would set up an independent new federal privacy commission to study things like the control of Social Security numbers and to receive complaints about government invasions of privacy. This is strongly opposed by the administration. Whether the House will go along with creation of such a commission is perhaps the main unresolved feature of the privacy bill.

In all, it's a fairly modest piece of legislation, compared with the heat of the rhetoric about protecting privacy. The bill won't really require federal agencies to make any big retrenchment in their current data-collecting. "I don't think it's going to stop them from doing what they're doing now, observes Douglass Lea director of the American Civil Liberties Union Privacy Project.

But Mr. Lea and some Congressmen say a hold-the-line bill is especially timely. Coming for sure are new generations of computers to handle national health insurance records, the files of a revamped welfare system and expanded criminal records. Columbia's Professor Westin argues that both government question-askers and computer engineers need firm privacy-protection ground rules now, before all those new questionnaires and computers are designed.

Senators Charles Percy of Illinois and Barry Goldwater of Arizona also think it would be a good idea to hold the line now on the use of Social Security numbers. Though the Government Operations Committee shrank from ordering a rollback of traffic in Social Security numbers, the two Senators intend to offer on the Senate floor an amendment that would allow government and business data banks to keep using the unmbers if they're doing so now, but to prevent any new users from discriminating against people who wont give out their numbers. The amendment, for example, would forbid a phone company from trying to enforce any new data system based on Social Security numbers by charging a higher fee to an uncooperative customer.

Hold-the-line tactics like that, says the ACLU's Mr. Lea, will at least make government and business data planners think anew about the easy drift toward universal numbers that "make it easy to do a full field check." And he thinks the pending bill at least will let more people challenge the sometimes casual way the bureaucracy throws questions at people for no very good reason.

"It's the beginning of a process of democratizing the way the government collects its infromation," he says. "At some point somebody's going to be able to use this law by telling an agency: 'Hey, you don't need that doggoned data. Cut it out.'"

[From the Wall Street Journal, Dec. 19, 1974]

Congress Finishes Work on "Privacy" Bill But Measure Has a Number of Loopholes

(By Arlen J. Large)

Washington.—Congress finished work on a "privacy" protection bill that reflects the federal bureaucracy's ability to defuse legislation that threatens it.

The final bill also withdraws a proposed barrier to the use of Social Security identifying numbers by banks and other private businesses, and it omits a mailing-list provision that was seen as a threat by commercial mailers, who lobbied hard against it.

The legislation, distilled from a flurry of initial ideas on how to protect the privacy of individuals from federal snoopers and data banks, by unanimous consent was given final approval by the House yesterday. The Senate passed it Tuesday by a vote of 77 to 8, with the opposition coming from members who thought the bill would hamper federal law enforcement. There was little complaining from the sponsors about how much the legislation had been watered down from earlier versions.

Both the House and Senate earlier had passed bills aimed at the same general objective: Every federal agency that operates a computer data bank or physical file containing information about individuals must publicly disclose that fact, and say what it's used for. Individuals then would have the right to inspect the file and make corrections, lest damaging falsehoods spread to other agency data banks or into computers outside the government.

The final compromise bill still makes that general requirement, and sponsors hope it will tighten up federal procedures for gathering and maintaining records about people. But the measure contains a number of loopholes insisted upon by federal agencies that feared a challenge to existing practices.

For example, the bill contains a general rule that one federal agency can't send data on an individual to another agency without that person's permission. However, there can be "routine" exchanges, such as giving government employes' names to the Treasury for paycheck purposes. The Internal Revenue Service

feared that earlier versions of the bill would keep it from exchanging income-tax data with state tax authorities. The IRS won assurances from Sen. Sam Ervin (D., N.C.), a principal sponsor, that the exchanges could continue.

The bill contains a broad exemption forbidding people to see data kept on them by federal law enforcement agencies. The FBI insisted on that, and it was worried about another proposal as well. An earlier version barred federal agencies to collect any information on how people exercise their First Amendment rights of free speech, religion and assembly, unless a statute requires it or an individual gives his permission. The FBI won the inclusion of an additional exemption for First Amendment surveillance that is "pertinent to and within the scope of an authorized law enforcement activity."

Earlier versions of the bill made a stab at controlling the use of Social Security numbers for identity purposes. In one of the few parts of the legislation affecting private business, it would have been illegal for anyone to discriminate against a person "in the course of any business or commercial transaction" because of his refusal to disclose his Social Security number. The provision was prompted by reports that some banks are enforcing their Social Security-based data systems by lodging penalty fees against customers who won dn't disclose their numbers.

The final bill omits this provision. However, it does retain a curb against the spread of Social Security number identity systems used by state and local governments. After next Jan. 1, state and local officials would be prevented from requiring people to give their Social Security numbers as a condition for registering a car, getting a driver's license, or voting in an election. Government identity systems in effect before Jan. 1 would be exempt from this rule, however.

An earlier version of the bill would have required business maintaining mailing lists to remove a person's name if he requested it in writing. This alarmed direct-mail advertisers, and the provision was removed from the final bill. Retained, however, was a prohibition against the sale or rental of mailing lists kept by federal agencies.

The original Senate bill would have set up a new five-member Privacy Protection Commission to investigate suspected violations of the new privacy law by federal agencies and draft privacy-protecting guidelines for federal officials to follow. The proposed commission was strongly opposed by the Ford administration.

The final bill sets up a seven-member Privacy Protection Study Commission to study privacy problems for two years. With that change, President Ford is expected to sign the bill.

[From the Columbia Human Rights Review, Vol. 4, No. 1 (1972)]

The First Amendment: A Living Thought in the Computer Age[1]

(By Sam J. Ervin, Jr.*)

Sherwood Anderson wrote words about America as true today as they were in the third decade of this century:

"America ain't cemented and plastered yet. They're still building it. . . . All America asks is to look at it and listen to it and understand it if you can. Only the understanding ain't important either; the important thing is to believe in it even if you don't understand it, and then try to tell it, put it down. Because tomorrow America is going to be something different, something more and new to watch and listen to and try to understand; and, even if you can't understand, believe."

Anyone seeking to understand contemporary America must deal with our national experience with computer technology. They must understand that it has become an essential tool in the "cementing and plastering" of our nation. They must understand that it has at once presented our country its greatest hope and its greatest challenge; keeping faith with our historical heritage and commitment to freedom, while enjoying the fruits of a rich industrialized society under a democratic constitution.

Throughout our nation the people involved with computer technology have charge of a great national resource which will affect the course of our economic

---

* U.S. Senator, North Carolina.

[1] Based on an address before the Spring Joint Computer Conference of the Federation of Information Processings Societies, Atlantic City, N.J., May 20, 1971.

and social progress. More important, insofar as it affects the exercise of governmental power and the power of large special interest groups, the new technology may help determine the course of freedom and human rights in our land.

In the process, I believe Americans could find wisdom in Sherwood Anderson's advice "to believe" in America. I say this because, as we grasp for the new computer technology and seek theories of systems analysis for our social problems, Americans may tend to forget to look to their own history. Some, in their haste to solve today's problems, may fear to translate America's promise of freedom into the program language of the computer age.

Those who are initiated into the technological mysteries of computer hardware and software may take great pride. Through their deeds and genius they have helped people go to the moon, produce music, create art, conduct off-track betting, run railroads, and administer welfare systems. They help maintain our national defense and they keep our economy running. They aid in catching criminals and they establish instant credit. They locate marriage-mates for people and they prejudge elections almost before the votes are cast.

A tape storage system has been described which will make it possible to store a dossier on every living person in the United States and to retrieve any one of them in a maximum of 28 seconds. With such feats to their credit, these people know better than anybody that in the application of their knowledge, they plan a major role in the economic and social well-being of our society. They are responsible for bringing to our nation all the wondrous blessing of computer technology, especially scientific methods of processing information.

They can bend these machines to their will and make them perform feats undreamed of ten or even five years ago.

They have a special understanding of the new information flow charts for the vast data systems in our government.

They hold the access code to control over the technology as it affects the individual in our society.

They may hold the key to the final achievement of the rule of law which is the promise of our constitution.

With this body of knowledge, therefore, they bear special responsibility for the preservation of liberty in our country. That they have accepted this responsibility is clear from the *Privacy* themes of many recent conferences of computer professionals, equipment manufacturers, and computer users in the governmental and private sectors.

Their power is not limited to their technical expertise, but is augmented by the sheer numbers in the computer-related professions.

Advertisements on TV, radio, in newspapers, and even on buses daily remind the public of the inducements and rewards of a career in computer and data processing fields.

In the Federal Government, their numbers are growing. An inventory of automatic data processing equipment shows that in 1952 there were probably two computers in government. In 1971, there were 5,961.[2]

In 1960, there were 48,700 man-years used in federal automated data processing functions. This includes systems analysis and design, programming, equipment selection and operation, key punching, equipment maintenance and administrative support. In 1970, there were about 136,504 man-years used in direct ADP work.

A recent illuminating report by the National Association for State Information Systems shows that in 35 states in 1971, over twenty-four and a half thousand people were engaged in ADP. Twenty-eight states together spent 181 million dollars of their budgets on such personnel.[3]

To glance through their professional journals, newspapers and bulletins each month is to be constantly amazed at the breadth and reach of the theories and

---

[2] Inventory of Automated Data Processing Equipment in the United States Fiscal Year 1971, General Services Administration, at 15. A report providing information on the digital electronic computers installed throughout the U.S. Government, which defines "computer" as a configuration of EDPE components which includes one central processing system concept which recognizes the growing importance of configurations with more than one central processing unit. This report responds to requirements of P.L. No. 89-306, Stat. (Oct. 30, 1965) and S. Doc. No. 15 (1965), Report to the President on the Management of Automatic Data Processing in the Federal Government.

[3] 1970 NASIS Report, Information Systems Technology in State Government at 18, developed by the State of Illinois and the National Association for State Information Systems, Council of State Governments.

accomplishments.[4] It also deepens a layman's wonder at the complex language which sometimes defies translation into ordinary English.

For all of these reasons, the general public stands in superstitious awe of the skills and knowledge, the machines and instruments, and the products derived and transmitted by them. For the uninitiated, the computer print-out bears a mystique and an aura of scientific rationality which makes it appear infallible. This is true for most lawyers and probably for most people in political life.

There is a theory abroad today in academic circles that America is divided into two worlds. One of them is the world of science and technology,[5] inhabited by people who are part of a technological and electronic revolution. In the other world are said to live all the rest of the people whose ideas and values are based on an earlier age.

In accordance with their theory, some have tried to stamp the scientist with motives and values different from those of other Americans; with goals oriented only toward efficiency or shorn of compassion, or, alternatively, with exclusive ability to determine social priorities. I cannot agree with this analysis, for I believe there is a yearning in every human heart for liberty, and for the freedom to express oneself according to the dictates of conscience. Despite a man's commitment to a chosen profession, he wants the freedom to fulfill himself as an individual and to use his God-given faculties free from the coercion of government.

So I do not believe Americans dwell in two worlds. Regardless of our origins, I believe we share a common heritage and a common destiny in that we are all engaged in searching for freedom. We share, according to the mandates of the Constitution, a common understanding that the best protection for that freedom rests on the limitations on the power of government and on the division of that power.

I cannot agree with such an analysis for another reason. Since the Senate Constitutional Rights Subcommittee began its study of computers, data banks and the Bill of Rights, I have received many letters from computer specialists, systems designers, engineers, programmers, professors and others in the scientific community which prove that despite, and perhaps because of their professions, they share the same concern about invasion of privacy as all other Americans, the same apprehensions about excesses of governmental surveillance and inquiries. Above all, they realize, perhaps better than others, that while the information technology they deal with can extend the intellect of man for the betterment of society, it also extends the power of government a million-fold.[6]

It makes it possible for government to administer more efficiently and to offer vastly better services to the taxpayers.

At the same time, it extends and unifies official power to make inquiries, conduct investigations, and to take note of the thoughts, habits and behavior of individuals. Of course, government has always had such power, but on a much smaller scale than today. Similarly, men possessing the power of government have always had the capacity for bad motives, simple errors or misguided purpose. There have always been problems with errors in the manual files. Now, computers may broadcast the image of these errors throughout a national information system.

What the electronic revolution has done is to magnify any adverse affects flowing from these influences on the life of the individual and on his proper enjoyment of the rights, benefits and privileges due a free man in a free society.

I reject the notion of division of Americans on the basis of scientific and technological values. If I had the unhappy and well-nigh impossible task of distinguishing two types of Americans, I believe I would distinguish between those

---

[4] See generally Computerworld (a weekly periodical servicing the computer community): Datamation: Data Management; and Business Automation.

[5] See, e.g., Brezezinksi, Between Two Ages, America's Role In the Technotronic Era, although all authors do not engage in such distinctions with the same judgments or purposes.

[6] Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary, 92d Cong., 1st Sess. [Feb. 23, 25 and Mar. 2–4, 9–11, 15 and 17 (1971)] [hereinafter cited as as 1971 Hearings.] Testimony of Robert Bigelow, attorney, describing concern of professional computer organizations and press, *id.* at 680; Bibliography, lists of public discussions on privacy and computers in the United States and abroad, id. at 692 et se.; Testimony of professor Caxton Foster, University of Mass., Department of Computer and Information Sciences, *id.* at 707.

who understand the proper limits and uses of governmental power and those who do not.

However much we try to rationalize decisions through the use of machines, there is one factor for which the machine can never allow. That is the insatiable curiosity of government to know everything about those it governs. Nor can it predict the ingenuity applied by government officials to find out what they think they must know to achieve their ends.

It is this curiosity, combined with the technological and electronic means of satisfying it, which has recently intensified governmental surveillance and official inquiries that I believe infringe on the constitutional rights of individuals.

Congress received so many complaints about unauthorized government data banks and information programs that the Subcommittee undertook a survey to discover what computerized and mechanized data banks government agencies maintain on people, especially about their personal habits, attitudes, and political behavior. We have also sought to learn what government-wide or nation-wide information systems have been created by integrating or sharing the separate data bases. Through our questionnaire, we have sought to learn what laws and regulations govern the creation, access and use of the major data banks in government.[7]

The replies we are receiving are astounding, not only for the information they are disclosing, but for the attitudes displayed toward the right of Congress and the American people to know what Government is doing.

In some cases, the departments were willing to tell the Subcommittee what they were doing, but classified it so no one else could know.[8] In one case, they were willing to tell all, but classified the legal authority on which they relied for their information power.[9]

Some reports are evasive and misleading. Some agencies take the attitude that the information belongs to them and that the last person who should see it is the individual whom it is about.[10] A few departments and agencies effectively deny the information by not responding until urged to do so.[11]

They reflect the attitude of the Army captain who knew Congress was investigating the Army data banks and issued a directive stating:

"The Army General Counsel has re-emphasized the long-standing policy of the Executive Branch of the Government . . . that all files, records and information in the possession of the Executive Branch is privileged and is not releasable to any part of the Legislative Branch of the Government without specific direction of the President." [12]

So, on the basis of this study, and on the withholdings of information from the American people which the Subcommittee has experienced,[13] I have concluded that the claim of the Government departments to their own privacy is greatly overstated. The truth is that they have too much privacy in some of their information activities. They may cite the Freedom of Information Act [14] as authority for keeping files secret from the individual as well as from the Congress. They then turn around and cite "inherent power" [15] or "housekeeping authority" [16]

---

[7] For a sample of questionnaire sent to all agencies and departments with slight alterations, see Letter to Secretary of Defense Melvin Laird, July 20, 1970 1971 Hearings at 1182, and to Attorney General Mitchell, June 9, 1970. Id. at 1212.

[8] See, e.g., State Department response to questionnaire, concerning its "Lookout File." See Letter of Sept. 9, 1970 to Subcommittee Chairman from Assistant Secretary of Defense Robert Moot, and list of classified enclosures, 1971 Hearings at 1186.

[9] Navy Department response, Aug. 13, 1970, citing a Roosevelt Executive memorandum assigning responsibilities for intelligence activities. Id. at 1201.

[10] Department of Transportation response. Testimony of Secretary Volpe. Id. at 720. Many other agencies will inform the individual of the general contents of his life, if he is denied some right, benefit or privilege and regulations permit a hearing or right of confrontation or cross-examination—but not before.

[11] Department of Health, Education, and Welfare, series of letters over a two year period on file with Subcommittee, and as of March, 1972, no response has been received containing substantive answers.

[12] Directive, ICGP–G–S3, Jan. 9, 1971, Release of Official Information to Legislative Branch of Government. 1971 Hearings, at 1179.

[13] Ervin, Secrecy in a Free Society, 213 Nation 454 (1971). See generally Hearings on Executive Privilege Before the Subcomm. on Separation of Powers of the Senate Comm. on the Judiciary, 92d Cong., 1st Sess. (1971). Testimony by Senator Tunney at 381 and William Rehnquist at 420.

[14] 5 U.S.C. § 552 (1970).

[15] See, e.g., 1971 Hearings, at 375, 431, 385. Testimony of Assistant Secretary of Defense Froehlke. Id. at 602, 599; testimony of Assistant Attorney General Rehnquist, note 13, supra.

[16] See, e.g., Justice Department response to Subcommittee questionnaire.

as a reason for maintaining data banks and computerized files on certain individuals; or they may cite the conclusions of independent Presidential factfinding commissions.[17]

So far the survey results show a very wideranging use of such technology to process and store the information and to exchange it with other federal agencies, with state and local governments and, sometimes, with private agencies.

Most of this is done in connection with administration of Government's service programs. However, a number of these data banks and information programs may partake of the nature of largescale blacklists. This is so because they may encompass masses of irrelevant, outdated or even incorrect investigative information based on personalities, behavior and beliefs. Unwisely applied or loosely supervised, they can operate to deprive a person of some basic right.

For instance, Federal Communications Commission response[18] shows that the FCC uses computers to aid it in keeping track of political broadcast time, in monitoring and assigning spectrums, and in helping it make prompt checks on people who apply for licenses. The Commission reported that it also maintains a Check List, which now has about 10,900 names. This Check List, in the form of a computer print-out, is circulated to the various Bureaus within the Commission. It contains the names and addresses of organizations and individuals whose qualifications are believed to require close examination in the event they apply for a license. A name may be put on the list by Commission personnel for a variety of reasons, such as a refusal to pay an outstanding forfeiture, unlicensed operation, license suspension, the issuance of a bad check to the Commission or stopping payment on a fee check after failing a Commission examination.

In addition, this list incorporates the names and addresses of individuals and organizations appearing in several lists prepared by the Department of Justice, other Government agencies, and Congressional committees. For example, the list contains information from the "FBI Withhold List," which contains the names of individuals or organizations which are allegedly subversive, and from the Department of Justice's "Organized Crime and Racketeering List," which contains the names of individuals who are or have been subjects of investigation in connection with activities identified with organized crime. Also included in the list are names obtained from other Government sources, such as the Internal Revenue Service, the Central Intelligence Agency, and the House Committee on Internal Security. According to the Commission, the use of the data arose in 1964 because during the course of Senate Hearings chaired by Senator McClellan, it was discovered that a reputed racketeering boss in New Orleans, Louisiana, held a Commission license. In order that such licensing not take place in the future, the Commission established liaison with the responsible divisions within the Department of Justice to be kept current on persons who might have such affiliations.

The Civil Service Commission maintains a "security file" in electrically powered rotary cabinets containing 2,120,000 index cards.[19] According to the Commission, these bear lead information relating to possible questions of suitability involv-

---

[17] For Defense Department reliance on the findings of the National Advisory Commission on Civil Disorders (Kerner Commission), see testimony of Assistant Secretary of Defense Froehlke, 1971 Hearings, at 379; noting the Commission's finding that the "absence of accurate information, both before and during disorder, has created special control problems for police," and the recommendation that "Federal-State planning should ensure that Federal troops are prepared to provide aid to cities. . . ."

The Department also cited a report filed by Corpus Vance following the Detroit 1967 disturbances, 1971 Hearings, at 378.

For law enforcement reliance on the Kerner Commission and similar commissions, see e.g., testimony of Richard Velde for the Law Enforcement Assistance Administration, 1971, Hearings at 608:

Several States also developing with LEAA funds information systems related to civil disorders. Most of these systems have as their objective either tension detection and forecasting or providing support to tactical units. It should be noted that the Kerner Commission studied this problem carefully and recommended that the police develop adequate intelligence for tension-detecting as well as on-the-scene information for tactical units. Many of the systems LEAA supports in the civil disorders area arose out of the recommendations of the Kerner Commission and similar commissions established by the States.

For reliance on Warren Commission finding of information gaps, see response to Subcommittee questionnaires by the Secret Service, Nov. 21, 1969, reprinted at 115 Cong. Rec. 39,114 (1969), and by the State Department Jan. 4 and Mar. 10, 1970; both responses in Subcommittee file.

[18] Response to questionnaire, in Subcommittee files, Mar. 25, 1971.

[19] Id. Aug. 18, 1970.

ing loyalty and subversive activity. The lead information contained in these files has been developed from published hearings of Congressional committees, State legislative committees, public investigative bodies, reports of investigation, publications of subversive organizations, and various other newspapers and periodicals. This file is not new, but has been growing since World War II.

The Commission chairman reported:

"Investigative and intelligence officials of the various departments and agencies of the Federal Government make extensive official use of the file through their requests for searches relating to investigations they are conducting."

In another "security investigations index" the Commission maintains 10,250,000 index cards filed alphabetically covering personnel investigations made by the Civil Service Commission and other agencies since 1939. Records in this index relate to incumbents of Federal positions, former employees, and applicants on whom investigations were made or are in process of being made.

Then, the Commission keeps an "investigative file" of approximately 625,000 file folders containing reports of investigation on cases investigated by the Commission. In addition, about 2,100,000 earlier investigative files are maintained at the Washington National Records Center in security storage. These are kept to avoid duplication of investigations or for updating previous investigations.

The Housing and Urban Development Department is considering automation of a departmental system which would integrate records now included in FHA's Sponsor Identification File, Department of Justice's Organized Crime and Rackets File, and HUD's Adverse Information File.[20] A data bank consisting of approximately 325,000 3 x 5 index cards has been prepared covering any individual or firm which was subject of or mentioned prominently in, any investigations dating from 1954 to the present. This includes all FBI investigations of housing matters as well.

In the area of law enforcement, the Bureau of Customs has installed a central automated data processing intelligence network which is a comprehensive data bank of suspect information available on a 24-hour-a-day basis to Customs terminals throughout the country.[21]

According to the Secretary of the Treasury:

"These records include current information from our informer, fugitive and suspect lists that have been maintained throughout the Bureau's history as an enforcement tool and which have been available at all major ports of entry, though in much less accessible and usable form. With the coordinated efforts of the Agency Service's intelligence activities, steady growth of the suspect files is expected."

There is the "Lookout File" of the Passport Office and the Bureau of Security and Consular Affairs.[22] This computerized file illustrates the "good neighbor" policy agencies observe by exchanging information in order to keep individuals under surveillance for intelligence and law enforcement purposes. Maintained apart from the twenty million other passport files, its basic purpose is to assist in screening passport applicants to make certain they are citizens of the United States and that they are eligible to receive passports. Requests for entry into this system are received from component agencies of the Department, from other government agencies, or in the limited category of child custody, from an interested parent or guardian.

The Department assured the Subcommittee that data recorded in this "Lookout File" is not disseminated. Rather, it serves as a "flag" which, if a "hit" or suspect is recorded, is furnished to the original source of the lookout and consists of the name of the individual and the fact that he has applied for a passport. The individual is not told that he is in the file until the information is used adversely against him. Then, according to the report, "he is fully informed and given an opportunity to explain or rebut the information on which the adverse action is based."

Among some of the reasons listed for people being in the Lookout File are the following:

If the individual's actions do not reflect to the credit of U.S. abroad:

---

[20] Id. June 22, 1970.
[21] Id. May 28, 1970.
[22] Id. Jan. 4, 1970.

If he is wanted by a law enforcement agency in connection with criminal activity;

If a court order restricting travel is outstanding or the individual is involved in a custody or desertion case;

"If he is a known or suspected Communist or subversive;

"If he is on the Organized Crime and Rackets List or is a suspected delinquent in military obligations."

The Defense Industrial Security Clearance Office is preparing to computerize its card files on over one and a half million private citizens who are employees of businesses doing classified contract work for the Federal Government.[23]

The Federal Deposit Insurance Corporation maintains information on people now associated with banks insured by the FDIC or who have been associated with such banks in the past.[24] It keeps a file on the names of individuals gained from newspapers and other public sources if they are characterized as having an unsatisfactory relationship with any insured bank or any closed insured bank. This also includes information supplied to the Corporation by other investigative or regulatory agencies on persons connected with an insured bank.

The Army maintains the U.S. Army Investigative Records Repository (USAIRR) which contains about 7,000,000 files relating principally to security and criminal investigations of former and present members of the Army, civilian employees and employees of private contractors doing business with the Army. The other services maintain similar investigative files.[25]

There is a Defense Central Index of Investigation operated by the Army for the entire Defense Department. The Index is designed to locate any security or criminal investigative file for any Defense agency and will be computerized shortly. It contains identifying data such as name, date of birth and social security number on people who have ever been the subject of investigations.[26]

There are all the data banks and computers in the Department of Justice[27] for intelligence, for civil disturbance prevention; for "bad checks passers;" for organized crime surveillance; and for federal-state law enforcement cooperation through the computerized National Crime Information Center.

On the basis of our investigation of complaints reviewed by Congress,[28] I am convinced that people throughout the country are more fearful than ever before about those applications of computer technology and scientific information processing which may adversely affect their constitutional rights. Furthermore, my study of the Constitution convinces me that their fears are well founded.

First, they are concerned that through a computer error they may be denied basic fairness and due process of law with respect to benefits and privileges for which they have applied.

---

[23] Id. Aug. 1970. See also 1971 Hearings, at 375, Froehlke testimony on this and other Defense Department records systems.

[24] Response to questionnaire, Feb. 22, 1972. See also 12 U.S.C. § 1811 et seq. (1964), Amendments to Federal Deposit Insurance Act, requiring bank recording and reporting to Internal Revenue Service transactions, S. Rep. 91–1139 and H.R. Rep. 91–975.

[25] See note 23 supra.

[26] Response to Subcommittee questionnaire, Aug. 1970. Also described in Froehlke testimony, note 23, supra and in Army Undersecretary Beal letter of Mar. 20, 1970, reprinted in 1971 Hearings, Part II at 1051, and at 116 Cong. Rec. 26327–51 (1970).

[27] For descriptions and citations to supporting statutes and regulations, see response to Subcommittee questionnires, 1971 Hearings, Part II at 1312–68. See also discussion in testimony of Justice Department officials. Id. Part I at 597, 849.

[28] For descriptions and summaries of some of these complaints and concerns, Remarks of Senator Ervin, 116 Cong. Rec. 30,797, 41,751, 43,944 and 117 Cong. Rec. S. 985 (daily ed. Feb. 8, 1971). In particular, note opening statements by Subcommittee Chairman each day of 1971 Hearings outlining issues of concern for the day. Of interest here is a Dec. 1971 report, A National Survey of the Public's Attitude Toward Computers, sponsored by the American Federation of Information Processing Societies and Time Magazine noting that:

> There is major concern about the use of large computerized information files. Thirty-eight percent of those surveyed believe computers represent a real threat to people's privacy as opposed to fifty-four percent who disagreed. Sixty-two percent are concerned that some large organizations keep information about millions of people. In addition, fifty-three percent believe computerized information files might be used to destroy individual freedoms; fifty-eight percent feel computers will be used in the future to keep people under surveillance; and forty-two percent believe there is no way to find out if information about you stored in a computer is accurate. In general, the public believes government should make increased usage of computers in a number of areas, that such usage will make government more effective, and that there will, and should be, increasing governmental involvement in the way computers are used.

Secondly, they are concerned about illegal access and violation of confidentiality of personal information which is obtained about them by government or industry.

These are actions which for any one individual or for entire groups may lead to a loss of the ability to exercise that "pursuit of happiness" which the Declaration of Independence declares is one of the unalienable rights of man.

These are actions which, by producing erroneous reports, may limit or deny a person's economic prospects and thereby impair that liberty which under the 5th and 14th amendments government may not impair without due process of law.

ARREST RECORDS

This possibility is illustrated by a letter [29] I received from a man who describes the effect on his life of an incident which occurred when he was fifteen years of age. In connection with a locker theft, he was taken to the police station, finger-printed, questioned and then he left, cleared of charges. He was not involved in any incident subsequently except a few minor traffic violations. He served 11 years in the armed services and held the highest security clearances. After gaining employment with a city government, he discovered that the youthful incident was, 15 years later, part of an FBI file and distributed to employers on request. He was asked to explain the incident for personnel records and to state why he withheld the information. Although he was unaware of the record, he believes the failure to list the incident was a factor in not gaining employment in several instances, and he was told he would have to institute court action to have the record expunged.

The problem he and millions of others face with respect to their records is illustrated by a regulation issued by the Attorney General last year restating the goal of the Federal Bureau of Investigatino "to conduct the acquisition, collection, exchange, classification, and preservation of identification records . . . on a mutually beneficial basis." [30] Among the agencies listed as eligible to receive and supply information were railroad police, banking institutions and insurance companies.

In Washington, D.C., a young man who was an innocent bystander during a campus demonstration was arrested by police and then released. Knowing that the FBI could distribute such records to employers, he hired a lawyer and spent large sums of money in a suit to have his arrest record expunged. The lower court denied his request, but the Court of Appeals ruled that, in the District of Columbia at least, arrest records should be expunged for innocent bystanders caught up in mass police arrests.[31]

In another case, a young man was arrested on probable cause and fingerprinted in California. When the police could not connect him with the case, he was released. He sought to have his arrest record expunged, or alternatively, to have strict limitations placed on its dissemination to prospective employers and others by the Federal Bureau of Investigation. While the U.S. District Court denied his request for expungement, it did say that his arrest record may not be revealed to prospective employers except in the case of any Federal agency when he seeks employment with that agency. However, it could be distributed for law enforcement purposes. Congress later restored this power to the FBI temporarily in an annual appropriation bill.

---

[29] Letter, identity withheld, in Subcommittee files with comment by the Director of the Federal Bureau of Investigation.

[30] 28 C.F.R. § 0.85 (b) ; codifying rulings by the Attorney General pursuant to 28 U.S.C. § 534 which provides :

(a) The Attorney General shall—

(1) acquire, collect, classify, and preserve identification, crime and other records ; and exchange these records with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions.

(b) The exchange of records authorized by subsection (a) (2) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

(c) The Attorney General may appoint officials to perform the functions authorized by this section.

[31] Morrow v. District of Columbia, 417 F. 2d 728 (D.C. Cir. 1969). For a summary of case law on this subject, see Longton, Maintenance and Dissemination of Records of Arrest Versus the Right to Privacy, 17 Wayne L. Rev. 995 (1971).

Judge Gesell's comments in this case of *Menard* v. *Mitchell*[32] are significant for the issue of arrest records, but also for the Army's computer surveillance program and for many other government intelligence systems now being designed. He stated that while "conduct against the state may properly subject an individual to limitations upon his future freedom within tolerant limits, accusations not proven, charges made without supporting evidence when tested by the judicial process, ancient or juvenile transgressions long since expiated by responsible conduct, should not be indiscriminately broadcast under governmental auspices." He also said:

"The increasing complexity of our society and technological advances which facilitate massive accumulation and ready regurgitation of farflung data have presented more problems in this area, certainly problems not contemplated by the framers of the Constitution. These developments emphasize a pressing need to preserve and to redefine aspects of the right of privacy to insure the basic freedoms guaranteed by this democracy.

"A heavy burden is placed on all branches of Government to maintain a proper equilibrium between the acquisition of information and the necessity to safeguard privacy. Systematic recordation and dissemination of information about individual citizens in a form of surveillance and control which may easily inhibit freedom to speak, to work, and to move about in this land. If information available to Government is misused to publicize past incidents in the lives of its citizens the pressures for conformity will be irresistible. Initiative and individuality can be suffocated and a resulting dullness of mind and conduct will become the norm. We are far from having reached this condition today, but surely history teaches that inroads are most likely to occur during unsettled times like these where fear or the passions of the moment can lead to excesses."

There are many similar cases pending throughout the states. Present laws are not sufficient to assure that an individual will be judged on his merit and not by inaccurate arrests records distributed by a national law enforcement computer.[33]

---

[32] Menard v. Mitchell, 430 F. 2d 486 (D.C. Cir. 1970), decision upon remand, 328 F. Supp. 718 (D.D.C. 1971). The Court construed 28 U.S.C. § 534 narrowly to avoid the constitutional issues raised by Menard and found that:

It is abundantly clear that Congress never intended to, or in fact did, authorize dissemination of arrest records to any state or local agency for purposes of employment or licensing checks.

It found certain faults with the present system: (1) State and local agencies receive criminal record data for employment purposes whenever authorized by local enactment, and these vary state by state and locality by loyality. (2) The Bureau cannot prevent improper dissemination and use of the material it supplies to hundreds of local agencies. These are no criminal or civil sanctions. Control of the data will be made more difficult and opportunities for improper use will increase with the development of centralized state information centers to be linked by computer to the Bureau. (3) The arrest record material is incomplete and hence often inaccurate, yet no procedure exists to enable individuals to obtain, correct or supplant the criminal record information used against them, nor indeed is there any assurance that the individual even knows his employment application is affected by an FBI fingerprint check.

The Court invited Congressional action, noting that: with the increasing availability of fingerprints, technological developments, and the enormous increase in population, the system is out of effective control. The Bureau needs legislative guidance and there must be a national policy developed in this area which will have built into it adequate sanctions and administrative safeguards.

[33] Congressional response to the District Court's invitation has taken several forms, among them, a bill, S. 2545, introduced, but not acted on, to authorize the Attorney General to exchange criminal record information with certain state and local agencies. Remarks by Senator Bible, S. 14558, 117 Cong. Rec. (daily ed. Sept. 20, 1971); and an amendment to the Department of Justice Appropriation Act of 1972 temporarily restoring the power over arrest records limited by the Menard decision. 117 Cong. Rec. S. 20461 (daily ed. Dec. 3, 1971). House Judiciary Subcommittee No. 4 on Mar. 16 began hearings on H.R. 13315, a bill introduced by Rep. Edwards, "to provide for the dissemination and use of criminal arrest records in a manner that insures security and privacy."

A related, but more comprehensive bill, S. 2546, was introduced by Senator Hruska on Sept. 20, 1971, 117 Cong. Rec. (daily ed.) to insure the security and privacy of criminal justice information systems. This is termed the Attorney General's response to an amendment to the Omnibus Crime Control Act of 1970, 18 U.S.C. §§ 351, 1752, 2516, 3731 (1964), requiring the Law Enforcement Assistance Administration to submit legislative recommendations to promote the integrity and accuracy of criminal justice data collection. LEAA demonstrated a prototype computerized system for exchange of criminal history information with the states, a project known as SEARCH—System for Electronic Analysis and Retrieval of Criminal Histories. In Dec. 1970, Project SEARCH was turned over to the FBI for the development of an operation system to be part of the National Crime Information System. The bill deals with criminal offender record information as well as criminal intelligence information.

A discussion of the philosophical, constitutional and legal issues and problems related to such a computerized system is found, with bibliographies, in Security and Privacy Consideration in Criminal History Informaton Systems, Technical Rept. No. 2, July, 1970,

Such threats to privacy and liberty arise with special force in the area of intelligence records. The Subcommittee study reveals two serious problems which have acquired national urgency through the introduction of computer technology. First, the problem of safeguarding intelligence information from improper release by government itself, and secondly, the problem of confining its collection to appropriate areas and subjects.

Government has, and should have, power to collect information, even raw, unverified intelligence information, in fields in which government has a lawful, legitimate interest. But this great power imposes a solemn responsibility to see that no one is given access to that information, except the Government itself for some legitimate purpose. There could never, for instance, be justification for Government to disclose intelligence gathered about citizens pursuant to its powers, to other citizens for their own personal or financial aggrandizement. Nor should Government through disclosure of confidential documents aid and abet the writing of sensational articles in private journals operated for commercial profit.

Nevertheless, the Subcommittee received testimony and evidence about two cases, which illustrate the misuse of confidential intelligence information for such purposes.

One involved a man in political life, the mayor of San Francisco, who was the subject of an article in Look Magazine purporting to establish that he associated with persons involved in organized crime. When the Mayor sued the magazine for libel, he undertook through subpoena power to learn the basis for such charges and where and how the authors obtained their information. He learned that they had received confidential information and documents from intelligence data banks. The information came from files and computer printouts of a number of major Federal, state and local government law enforcement agencies. They involved the U.S. Attorney General's Office, the Federal Bureau of Investigation, Internal Revenue Service, Federal Bureau of Narcotics, the Customs Bureau, the Immigration and Naturalization Service, the California Criminal Identification and Investigation Bureau, the California State Department of Justice, and the Intelligence Unit of the Los Angeles Police Department. By their own testimony for the case, the authors of the article admitted that they examined, obtained or borrowed originals or copies of such law enforcement records containing much raw unevaluated intelligence information on numerous people including the names of three U.S. Presidents, the state Governor, a number of Senators, and many private law-abiding citizens, not accused of any crime. These documents were obtainable despite the fact that many of them were stamped "Confidential" or "Property of U.S. Goevernment For official use only. May not be disseminated or contents disclosed without permission. . . ."

There is more about these and other disclosures in the hearing record, but I believe the Mayor's testimony [34] illustrates many of the dangers to privacy in this age of large investigative networks and instant computerized dossiers. It also illustrates the lack of sufficient criminal, civil, or administrative sanctions against unwarranted sharing and disclosure of such confidential information. To my knowledge, no punitive action was taken except for a disciplinary personnel action filed against an agent of the Federal Bureau of Investigation, who was then allowed to retire.

---

by Project SEARCH, California Crime Technological Research Foundation, funded by the Law Enforcement Assistance Administration, Department of Justice. Also pertinent is the testimony of LEAA officials on the use of information and intelligence systems by criminal justice agencies. 1971 Hearings, on the National Crime Information Center. Id. at 914.

For a model state act proposed for criminal offender record information, see generally Technical Memorandum No. 3, May 1971 by Project SEARCH.

As we have a highly mobile population, so we have a highly mobile criminal population, which requires that governments be able to share rapidly the information in their data banks in the interest of law enforcement. The problem is determining what agencies and what officials should control what information.

[34] See 1971 Hearings at 493–530, Testimony of Joseph Alioto, Mayor of San Francisco, and exhibits submitted. For response of Justice Department officials, see testimony of William Rehnquist, id. at 604, 878–88, and a series of memoranda from the Federal Bureau of Investigation, the Bureau of Narcotics and Dangerous Drugs, which memoranda were submitted by Assistant General Rehnquist with the caveat that.

Under the traditional notions of separation of powers, it seems to me probable that the Department could justifiably decline to furnish portions of this information . . . Id. at 1371.

The weakness of any applicable regulations is demonstrated by the report of the Bureau of Narcotics and Dangerous Drugs that its current disclosure order "would not cover the release of collateral intelligence information, information contained in dead files, or information on nondefendants, such as that disclosed in the Alioto testimony." The Bureau further stated that under the provisions of its new Agents Manual it is only a "breach of integrity" to make unauthorized disclosure of files which are restricted to official use.[35]

MISUSE OF MILITARY INTELLIGENCE RECORDS

Another case[36] illustrates how the Army's investigative intelligence services and files were put to private use to obtain the dismissal of an employee of a private business. In this instance an Army intelligence agent whose routine duties involved security investigations and surveillance for the Army's civil disturbance prevention program described to the Subcommittee how he was ordered by his superiors to conduct an investigation of the bank loan records, police and court records of the private citizen and was told to give the resulting information to the employee's supervisor. He later learned that the investigation had been ordered by an intelligence officer as a personal favor for an official of the company. When the agent reported this to his superiors, he was told in a classified letter that the matter involved "national security." A year later, following his separation from the service, the agent reported the incident to the Inspector General of the Assistant Chief of Staff for the Pentagon, who began an investigation. All of his allegations were confirmed and firm disciplinary actions were taken against the guilty officers. It was too late, however, for the subject of the Army investigative report, who had already been dismissed.

These cases illustrate the concerns over political administrative and technical problems of access, confidentiality and purging of erroneous or outdated records in computer systems. But these are issues which have long concerned legislatures, bar associations and others.

The major reason for public apprehension about computer technology and information sciences is the use of them to acquire, process, analyze and store information about activities and matters which are protected by the First Amendment.

What people writing to Congress fear most is the uses to which this technology may be put by men of little understanding but great zeal. They know that, applied to unlawful or unwise programs, computers merely absorb the follies and foibles of misguided politically-minded administrators.

In Federal Government, the new technology, combined with extended Federal-state services and their spin-off information systems, have produced vast numbers of investigators, analysts, and programmers devoted to the study of people and society. With the zeal of dedicated civil servants, they are devoted to the building of data bases on the habits, attitudes and beliefs of law-abiding citizens. Much of what they gather is trivial; much of it goes far beyond the needs of government. Some of it is shared extensively and often unnecessarily by agencies who are components of these large information systems.

People seeking government jobs in some agencies are told to reply to personality tests asking:

I believe there is a God.

I believe in the second coming of Christ.

I believe in a life hereafter.

---

[35] 1971 Hearings, Part II at 1375. In his memorandum of Mar. 5, 1971, the Director of the Bureau of Narcotics and Dangerous Drugs noted ". . . it is possible that the documents or information in these four exhibits could have been passed to the LOOK reporters by a BNDD employee." He cites BNDD Order 0-98, May 27, 1970 as the Bureau's current public information policy and as essentially a restatement of 28 C.F.R. Pt. 50, § 50.2, which covers the dissemination of most types of information for the Department. However, he states that the strongest applicable regulations in this matter are found in 28 C.F.R. Pt. 45, § 45.735: "No employee shall use for financial gain for himself or for another person, or make any other improper use of, whether by direct action on his part or by counsel, recommendation, or suggestion to another person, information which comes to the employee by reason of his status as a Department of Justice employee and which has not become part of the body of public information."

Obviously, the disclosure of documents stamped "For official use only" would be contrary to this regulation if, in fact, the disclosures were made by Department of Justice employees.

[36] For statement submitted by a Special Agent of Military Intelligence and related correspondence, see 1971 Hearings, Part II at 1451–1457.

I am very religious (more than most people).
I go to church almost every week.
I am very strongly attracted by members of my own sex.
I love my father.
My sex life is satisfactory.
Once in a while I feel hate toward members of my family whom I usually love.
I wish I were not bothered by thoughts about sex.

When the Subcommittee held hearings on these practices, government officials explained that there was no right or wrong answer to the questions, that the responses were coded and analyzed by the computer.[37]

I asked whether they did not think such inquiries violated the privacy of the individual's thought about matters that were none of the business of government. The reply was that there was no Supreme Court decision holding that people who apply for federal employment have a constitutional right to privacy.

There was a Civil Service program telling employees to fill out computer punch cards stating their racial, ethnic or national origin along with their social security number.[38] In the land renowned for being the "melting pot" of the world, over 3 million individuals had to analyze their backgrounds and reduce them to one of four squares on an IBM card. If they protested that these matters were none of the business of government, they were blacklisted in their offices and harassed with computer-produced orders to return the completed questionnaire. The resemblances between this program and those of totalitarian governments in our recent history were all too obvious.

The Census Bureau makes more use of computer technology for personal inquiries than anyone.[39] It conducts surveys for its own uses backed by the criminal and civil sanctions. One of these, the decennial census, asked people such questions as:

Marital Status: Now married, divorced, widowed, separated, never married.
(If a woman) How many babies have you ever had, not counting stillbirths?
Do you have a flush toilet?
Have you been married more than once?
Did your first marriage end because of death of wife or husband?
What was your major activity 5 years ago?
What is your rent?
What is your monthly electric bill?
Did you work at any time last week?
Do you have a dishwasher? Built-in or portable?
How did you get to work last week? (Driver, private auto; passenger, private auto; subway; bus; taxi; walked only; other means).

---

[37] See generally Hearings on Psychological Tests and Constitutional Rights Before the Subcomm. on Constitutional Rights of the State Comm. on the Judiciary, 89th Cong., 1st Sess. (1965) and Hearings on S. 3779 on Privacy and the Rights of Government Employees, 89th Cong., 2d Sess. (1969).

[38] See 1966 Hearings, supra note 37. In connection with a proposal introduced to protect the constitutional rights of employees of the executive branch and to prevent unwarranted governmental invasion of their privacy, see Senate remarks of Senator Ervin including discussion of need for law prohibiting requirements to reveal information on race, religion, national origin, personal family relationships, sexual attitudes and conduct and religious beliefs and practices in 112 Cong. Rec. 16081, 18634 (1966), 113 Cong. Rec. 4039, 10663, 27994 (1967), 114 Cong. Rec. 11235, 17161, 19613 (1968), 115 Cong. Rec. 2343, 117 Cong. Rec. (daily ed. Apr. 1 and May 11, 1971). By such legislation, government may be prevented from intruding into protected First Amendment areas on subjects which should have nothing to do with the operation of a civil service merit system. By exclusion of such sensitive, subjective information from the computer systems, initially, government will be precluded from basing individual or general social judgments on outdated standards, changing mores, variants in ethnic, cultural or geographical backgrounds, or previous conditions of the individual's mind, heart, and personality. It will necessarily be confined to a consideration of current information relevant and pertinent to the problem at hand.

[39] See generally Hearings on S. 1791 and Privacy, the Census and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Judiciary Committee, 91st Congr., 1st Sess. (1969) and hundreds of letters and complaints about coercive statistical questionnaires. Appendix also contains judicial, legal and constitutional research materials as well as examples of many social and economic questionnaires. See also Pine and Russell, Privacy: Establishing Restrictions on Government Inquiry, 18 Amer. Univ. L. Rev. 516 (1969). For a summary of the hearings, see Senate remarks of Senator Ervin, 115 Cong. Rec. 17718 (1969). For possible political uses of such information acquired as economic and social indicators, see Report by House Government Operations Committee, Subcommittee on Government Information, on Department of Labor briefings on economic statistics; and 23 Western Pol. Q. 235 (1970). See also the finding and recommendations on privacy and confidentiality of the President's Commission on Federal Statistics (1971).

How many bedrooms do you have?

Do you have a health condition or disability which limits the amount of work you can do at a job?

How long have you had this condition or disability?

Under even heavier sanctions, the Census Bureau puts questionnaires to farmers, lawyers, owners of businesses, and others, selected at random, about the way they handle their business and finances.[40]

The Census Bureau also makes surveys for many other departments and agencies.[41] For example, they put out statistical questionnaires which the Department of Health, Education, and Welfare wanted to send to retired people asking:

How often they call their parents;

What they spend on presents for grandchildren;

How many newspapers and magazines they buy a month;

If they wear artificial dentures;

"Taking things all together, would you say you're very happy, pretty happy, or not too happy these days?"

And many other questions about things on which government has no business demanding answers.

These people are not told that their answers are voluntary, but are harassed to reply and are given the impression they will be penalized if they do not answer.[42]

There are many other examples of inquiring social and economic data that are backed by the psychological, economic, or penal sanction of government. Clearly, Government has great need for all kinds of information about people in order to govern efficiently and administer the laws well; similarly, Congress must have large amounts of meaningful information in order to legislate wisely.

However, I believe these examples of governmental data collection illustrate my contention that the First Amendment wraps up the principle of free speech, which includes the right to speak one's thoughts and opinions as well as the right to be free of governmental coercion to speak them.

There are other examples of government programs which, well-meaning in purpose, are fraught with danger for the very freedoms which were designed to make the minds and spirits of all Americans free, and which work to keep

---

[40] See 1969 Hearings, supra note 39, testimony on behalf of the National Federation of Independent Business at 199, of attorney and farm owner William Van Tillburg at 74, W. Schliestett, businessman at 66, J. Cannon, attorney at 7,263.

[41] Id. at 830, Table of Census surveys of population and households, conducted for other government agencies, with indication of penalties and compliance techniques. In many of these, the data is kept on tape or film by both the Census Bureau and the sponsoring agency, and the confidentiality rules of the sponsoring agency apply.

[42] Id., at 251. Assistant Secretary of Commerce Chartener:

Assistant Secretary of Commerce Chartener. The wording deliberately has been rather subtle in its form. We never use the word "mandatory" on a questionnaire. Instead, people will be told that "your answer is required by law." In other cases, they may be told that a survey is authorized by law or it is important to your government or something of that sort. Now, the followup procedure is used not for purposes of coercion but rather in order to verify the correctness of an address.

Senator ERVIN. Do you not agree with me that such a procedure is designed to implant in the mind of the recipient of these questionnaires the impression that he is required by law to answer them?

Mr. CHARTENER. If it is a mandatory questionnaire that would be the case. In other instances, the repeated mailings which may go up to five or may involve telephone calls or even a personal call are simply a means of emphasizing the importance that the Government feels in getting this response . . .

The Department of Commerce opposed enactment of a simply-worded statute advising people that their responses to these statistical questionnaires were voluntary. Id. at 262.

Senator ERVIN. Would the Department of Commerce and its Bureau of the Census be opposed to enactment of Federal statutes which would require that the Bureau of the Census advise every citizen on a questionnaire sent out by the Bureau that where it is not required by law, not mandatory, this is an effort to elicit information desired by the Government on a voluntary basis?

Mr. CHARTENER. Senator, I think we would oppose that. This is a matter of rather subtle psychology. I do not think, personally, and this is the position of the Department, that we ought to go out of our way to tell people they do not need to bother filling out this questionnaire. . . .

Senator ERVIN. You think the statutes governing those questionnaires, which are mandatory and which are subject to the criminal penalty if not answered readily, are understandable by the average layman?

Mr. CHARTENER. I do not think any law is written to be readily understandable by the average layman. That is why we have lawyers.

But compare the testimony of the Secretary of the Department of Health, Education, and Welfare in the 1971 Hearings at 788, opposing legislation, but favoring administrative notice of voluntariness for that Department's forms.

America a free society. A number of these would be impractical, if not impossible, without the assistance of computer techology ad scientific data processing.

It is those First Amendment freedoms which are the most precious rights conferred upon us by our Constitution: the freedom to assemble peaceably with others and petition government for a redress of grievances; the freedom to worship according to the dictates of one's own conscience free of government note-taking; the freedom to think one's own thoughts regardless of whether they are pleasing to government or not; the freedom to speak what one believes whether his speech is pleasing to the government or not; the freedom to associate with others of like mind to further ideas or policies which one believes beneficial to our country, whether such association is pleasing to government or not.

THE SECRET SERVICE

In the pursuit of its programs to protect high government officials from harm and federal buildings from damage,[43] the Secret Service has been pressured to create a computerized data bank. Their guidelines for inclusion of citizens in this data bank requested much legitimate information but also called for information on "professional gate crashers;" "civil disturbances;" "anti-American or anti-U.S. Government demonstrations in the United States or overseas;" pertaining to a threat, plan, or attempt by an individual or group to "embarrass persons protected by the Secret Service or any other high U.S. Government official at home or abroad;" "persons who insist upon personally contacting high government officials for the purpose of redress of imaginary grievaces;" and "information on any person who makes oral or written statements about high government officials in the following categories: (1) threatening statements, (2) irrational statements, and (3) abusive statements."

Americans have always been proud of their First Amendment freedoms which enable them to speak their minds about the shortcomings of their elected officials. As one in political life, I have myself received letters I considered abusive. Similarly, I have uttered words which others have deemed abusive. While I am not a "professional gate crasher," I am a malcontent on many issues. I have written the President and other high government officials complaining of grievances which some may consider imaginary; and on occasion, I may also have "embarrassed" high government officials.

One man wrote me his concern about this program and commented:

"The Secret Service ought to go after my mother-in-law, too. On her last visit she said that the Vice President doesn't seem to have too many brains. She also said that Senator ——— has a face like a carbuncle. Should I report this to the Secret Service?[44]

There is no doubt that the physical protection of the President and high government officials is a legitimate government purpose and all reasonable means must be taken in pursuit of it. Nevertheless, such broad and vaguely worded standards for investigating and adversely reporting Americans to their government on the basis of their utterances could, at one time or another, include most members of Congress and most politically aware citizens. It could cover heated words exchanged in political debate and discussion anywhere in the country. Yet civil and military officials throughout the Federal government and in some local law enforcement agencies were requested to report people coming to their attention who were thought to fit these criteria.

The Subcommittee has not received complete answers to our questionnaire on the subject of this computer and the national reporting system it serves. However, we have indications that other broad and zealous information programs, including the Army civil disturbance system,[45] are sharing of feeding on entries which, if not carefully evaluated, may produce serious consequences for the rights and privileges of citizens. Illustrating the misunderstandings and misinterpretations possible is the fact that military doctors have expressed to me

[43] 115 Cong. Rec. 3356 (1969) and guidelines printed there. See also note 17, supra, correspondence and guidelines printed at 1541, 1971 Hearings, Part II. See remarks of Rep. Stanton, 118 Cong. Rec. at H208 (daily ed., Jan. 24, 1972). [Complaints Against Secret Service].

[44] Letter in Subcommittee files.

[45] See Department of the Army Civil Disturbance Information Collection Plan, May 2, 1969, collection priorities and requirements and distribution list for government agencies Printed in 1971 Hearings at 1126, 1136. This plan also appears with remarks of Senator Bayh, 117 Cong. Rec. 2290 (daily ed., Mar. 2, 1971).

their concern about an allegedly "secret" agreement between the Defense Department and the Secret Service which they were told was a recent one and which required reporting of all servicemen receiving administrative discharges. One psychiatrist writes of his concern for the confidentiality of medical records in such action:

"I see very little reason for this. My impression of the individuals whom I recommended for such a discharge was that these were immature individuals who were not able to adapt to the service for one reason or another. Not by any stretch of the imagination were these individuals unpatriotic or a threat to the security of the nation." [46]

When I asked the Secretary of the Navy about this, the Subcommittee was informed that a person is not reported to the Secret Service merely because he received an administrative discharge from the Navy or Marine Corps.[47] However, we were informed that pursuant to Naval regulations issued under a secret 1965 Agreement,[48] the Navy reports an average of 400 persons annually. We learned, for example, that among the many categories of people to be reported were not only servicemen but civilian employees of the Defense Department who were discharged on security or suitability grounds and who showed "evidence of emotional instability or irrational or suicidal behavior, expressed strong or violent sentiments against the United States," or who had "previous arrests, convictions, conduct or statements indicating a propensity for violence and antipathy for good order in Government." [49]

MILITARY SPYING

Another example of First Amendment information programs is the Army program for spying on Americans who exercised their First Amendment rights. Despite these rights, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.[50]

Allegedly, for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, tape-recorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

---

[46] Letters in Subcommittee files (identities withheld).

[47] Letter of inquiry from Subcommittee Chairman, July 6, 1971, citing the large number of reasons for which a person can receive an administrative discharge, ranging from family hardship to national security grounds, the inadequate procedures and safeguards surrounding such discharges, and the threat to individual freedom from unrestricted reporting of law-abiding citizens, who may become subjects of official surveillance through no fault of their own or of the Secret Service.

[48] This December 14, 1965 agreement between the Defense Department and the Secret Service was implemented within the Navy Department by SECNAV Instruction 5500.27, March 18, 1966, which contains a copy of the agreement. Administrative authority for this regulation is cited as Defense Dept. Directive 5030.34, dated Dec. 30, 1965; statutory authority for assistance to the Secret Service is cited as P.L. No. 90–331 (June 6, 1968) which provides for assistance to the Secret Service on request.

[49] Appendix B of Agreement. Under Appendix A, identification data, photograph, physical description, date and place of birth, employment, marital status and identifying numbers are to be furnished, together with summaries or exceprts from DOD files as applicable to an individual or group reported.

In a related exchange of correspondence, the Subcommittee Chairman, in response to complaints, directed an inquiry to the Secretary of the Navy, on April 22, 1970, about a Navy directive which required that in any case where enlisted personnel were to be separated under other than honorable conditions within the continental United States, local civil police authoritis were to be notified in advance of the name, race, sex and place and date of birth of the person, and of the time and place such separation is to be effected. This regulation seemed to serve no useful function since the Army and the Air Force functioned without one. On May 7, 1970, the Navy Department notified the Subcommittee that they concurred in this view and would delete the reporting requirement. (Correspondence in Subcommittee files.)

[50] For legal and constitutional implications, as well as a comprehensive historical account, see testimony of Christopher Pyle, an attorney and former Captain in Army Intelligence. See 1971 Hearings at 147, and exhibits providing examples of nation-wide military surveillance.

With very few, if any, directives [51] to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.[52]

The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks.[53]

The Army attempts to justify its surveillance of civilians by asserting that it was collecting information to enable the President to predict when and where civilians might engage in domestic violence, and that the President was empowered to assign this task to it by the statutes conferring upon him the power to use the armed forces to suppress domestic violence.

I challenge the validity of this assertion.

Under our system, the power to investigate to determine whether civilians are about to violate federal laws is committed to federal civil agencies, such as the FBI; and the power to investigate to determine whether civilians are about to violate state laws is reposed in state law enforcement officers.

If President Johnson believed he ought to have had information to enable him to predict when and where civilians might engage in future domestic violence, he ought to have called upon the FBI or appropriate state law enforcement officers for the information.

He had no power to convert the Army into a detective force and require it to spy on civilians.

This conclusion is made plain by the Constitution and every act of Congress relating to the subject. Sections 331, 332, 333 and 334 of Title 10 of the United States Code certainly did not confer any such power on the President. These statutes merely authorized him to use the armed forces to suppress domestic violence of the high degree specified in them, and conditioned their use for that purpose upon his issusing a proclamation immediately ordering the offenders "to disperse and retire peaceably to their abodes within a limited time."

The only other statute relevant to the subject is section 1385 of Title 18 of the Code, which prohibits the use of any part of the Army or Air Force "as a posse comitatus or otherwise to execute the law . . . except in cases and under circumstances expressly authorized by the Constitution or Act of Congress."

The legislative history of this statute is fully revealed in the opinion of United States District Judge Dooling in *Wrynn v. United States*, 200 F. Supp. 457 (E.D.N.Y. 1961). When the words of this statute are read in the light of its

---

[51] See Ervin, Privacy and Governmental Investigations, 1971 Univ. Ill L. Forum 137 (1971) for an account of the various plans and their lack of relevance to the problem of putting down civil disturbances, and for analysis of the Defense and Justice Department's claims to constitutionality for the actions of the military. Texts of four "plans," 1971 Hearings at 1123, 1119, 1154, 1731; Memorandum at 1139, 1141, 1278–98. Showing attempts by civilians to cut back on the program.

[52] The bulk of investigative activity by the Army's own personnel occurred at the field level. Agents collected information and filed "spot reports," "agents reports," and "summaries of investigation." Most of this data was forwarded up the chain of command but record copies were kept in data centers at every level of command. Manual files were maintained at every level. At least four and possibly more computer systems were employed to store, analyse and retrieve the information collected. Many files on lawful citizens were microfilmed and integrated with other files on persons who were suspected of violations of security and espionage laws. These computer systems were located in the headquarters of the Intelligence Command (Fort Holabird), the Continental Army (Fort Monroe), the Third Army Corps (Fort Hood), and in the Pentagon. More than one computer data bank was maintained in some of these locations. (Subcommittee investigation.)

[53] Testimony of Ralph Stein on the difficulty of labeling young people on the basis of their speech, when a difference of one digit was the difference between a communist and a non-communist, 1971 Hearings at 248, 260.

legislative history, it is obvious that the statute is not limited by the expression "as a posse comitatus or otherwise," but operates as a prohibition against the use of the Army to execute the laws without reference to whether it is employed as a posse comitatus or as a portion of the Army. Indeed, the statute embodies "the inherited antipathy of the American to the use of troops for civil purposes." [200 F. Supp. at 465].

President Johnson's use of the troops to spy on civilians, to build data banks and create computerized information systems, discloses that relevance of this statute to our day is sadly clear. Since neither the Constitution nor any Act of Congress expressly, or impliedly, authorized such use, the President was forbidden by section 1385 of Title 18 of the United States Code to use the Army to spy on civilians.

The Army's spying violated First Amendment freedoms of the civilians who became aware that they or the groups to which they belonged had been placed under surveillance. This is so because it undoubtedly stifled their willingness to exercise their freedom of speech, association and assembly.[54]

If any proof were needed of the logic and truth of this statement, it can be drawn from such testimony as the Subcommittee received from Dr. Jerome Wiesner who commented:

"Many, many students are fraid to participate in political activities of various kinds which might attract them because of their concern about the consequences of having a record of such activities in a central file. They fear that at some fuutre date, it might possibly cost them a job or at least make their clearance for a job more difficult to obtain." [55]

The Subcommittee has heard no testimony yet that the Army's information program was useful to anyone. The only result of the testimony by the Defense Department was to confirm my belief that under the Constitution and under the laws, the Army had no business engaging in such data-gathering and that the scope and breadth of the surveillance was so broad as to be irrelevant to the purpose.

Congress has still to discover the complete truth about these Army computers. Apparently, even officials responsible for intelligence did not know of the existence of the computers for implementing the program. The Subcommittee has repeatedly requested the testimony of the Army Generals who would be most knowledgeable about the computers and what they contained. We have just as repeatedly been

---

[54] See Brief for Respondents filed in Tatum v. Laird in the Supreme Court of the United States, No. 71-288, challenging the Army's surveillance program, and arguing that plaintiffs' claims are justifiable and ripe for adjudication; that the present inhibiting effect on the exercise of First Amendment rights creates a justifiable controversy; that the justiciablity of their claims is enhanced because the military exceeded its constitutional and statutory authority and intruded into civilian affairs; that they have standing to adjudicate these claims for themselves and the claims of others similarly situated; and finally, that they argue that their case cannot be mooted by the Army's assertion that its domestic surveillance activity has been reduced. The appendix contains an interesting and landmark study of the chilling effect of overbroad governmental programs on First Amendment activity from the social science view.

All of the plaintiffs named have been subjects of political surveillance, and all are believed to be subjects of reports, files, or dossiers maintained by the Army.

In an amici brief filed by Senator Ervin on behalf of the Unitarian Universalist Association, the Council for Christian Social Action, United Church of Christ, the American Friends Service Committee and the National Council of Churches of Christ, the question posed for review is framed as follows:

Do individuals and organizations not affiliated with the armed services present a justifiable issue under the First, Fourth, Fifth and Ninth Amendments when they allege that their rights of free expression, privacy and association have been infringed by unauthorized, unnecessary and indiscriminate military investigations of their political activities and personal lives? Brief for Respondents as amicus curiae at 7, Laird v. Tatum, No. 71-288 (1971).

Essential though the freedoms are, they are not easily exercised in a climate of fear, discord, and dissension, especially when the ideas being expressed are those which are displeasing to government and unsettling to the majority of citizens. . . . It is as such a time that the First Amendment is most necessary, most in danger, and most difficult to exercise. . . . The First Amendment however, was made for the timid as well as for the brave. While government cannot instill courage in the meek, it may not take advantage of a climate of fear to undertake a program which has the effect of restricting the First Amendment only to the very courageous. Government action, such as military surveillance, seemingly innocuous in the abstract, has the very real effect of suppressing the exercise of the First Amendment. The coercive power of this government action lies in the national climate of fear and doubt, and in the very real, tangible apprehension of some unknown form of retribution by government on those who it fears and therefore watches. That such apprehension exists in America today is manifest. Id. at 15.

[55] 1971 Hearings at 765.

denied their testimony as well as delivery and declassification of pertinent documents demonstrating the scope and purpose of the program.[56] The Army said it would cut back on the data-gathering on lawabiding citizens and would defer to the Department of Justice. So I asked the Justice Department officials how many computers that Department had containing information on people who lawfully exercised their First Amendment freedoms." [57]

I had seen newspaper articles quoting the director of the Justice Department's Interdivisional Information Unit. He said there that the computer's list of thousands of names is not a register of "good guys" or "bad guys." "It is simply a list of who participated in demonstrations, rallies and the like." This would include non-violent people as well as violent, he said.[58] On the basis of these reports, I asked for the testimony of this official, but for some strange reason, he could not be located.

Despite questioning during the hearings and correspondence with the Justice Department, we have been unable to obtain an accurate description of the use of Justice Department computers for collecting, processing and analyzing information on lawful First Amendment activities of citizens. Nor have we been able to ascertain or obtain the standards followed by the Department in deciding what individuals should be the subjects in such files, or how they should be excluded from such files.

LEGISLATIVE REMEDIES

There has been much discussion of the need for new laws granting access to individual records. I believe a person should have the chance to expunge, update and correct his records. With the advent of systematic record-keeping, a man needs the chance which a businessman has to go into economic bankruptcy and obtain a discharge from his past.

I believe, however, that we must go beyond that relationship between the individual and his records. We must act to restore a healthy balance to the relationship between the citizen and his government, and necessarily between Congress and the Executive Branch. Mere access to and knowledge of his individual file is not enough. Remedial action must be addressed to the curbing of the power of government over the individual and to restricting its power to deny information about government programs. The claim to an inherent power to monitor, investigate and compile dossiers on law-abiding citizens on the off-chance that they might need to be investigated for a legitimate governmental purpose at some time in the future must also be opposed.

As a result of the Subcommittee's experience in playing hide-and-go-seek with the Federal Government's computers and with the people who plan and supervise them, I am convinced these computers have too much privacy today. The Congress, the press and the public should have available an *habeas corpus* action for entire computer systems and programs themselves. No department should be able to hide such broad-based data programs and information systems. If they are lawful, the American people then have a right to full knowledge about the operation of their government. If they are not lawful and relevant for some purpose, they should be exposed for what they are—attempts to intimidate citizens into silence and conformity.

First, we need to devise some judicial remedy for confronting and testing the nature, purpose, legality and constitutionality of governmental data banks and large-scale intelligence information systems which by their very existence may threaten the quality of our First Amendment freedoms or whose contents may affect economic prospects, reputations or rights. Now pending before the United States Supreme Court is just such a challenge to the Army surveillance program and the military data banks, including at least four computer systems for storing and processing information on Americans across the land. [*Tatum* v. *Laird*, no. 71–288 (1971) (argued March 27, 1972)] The lower court denied standing to sue to plaintiffs who were subjects of surveillance and computer dossiers on grounds that they have not shown injury. [444 F.2d 947 (D.C. Cir. 1971)].

Congress must strengthen and enforce reporting requirements for computer systems. Not even in the audit of computers which the present law requires the General Services Administration to conduct each year is it possible for Congress,

---

[56] See exchange of correspondence on this subject. Id. Part II at 1046 A, 1180 Indices to letters.
[57] Id. at 597, 849.
[58] Id. at 616–62.

the press, and the public to get minimum information about all of the management uses of computers in government.

Secondly, I believe we must devise legal means of assuring the reporting of large government data banks to a central office established independently of the executive branch. This would require the filing of policy statements describing exactly what agencies feed a particular information system and who would receive or access data routinely from a particular data bank. These policy statements should be public records. In this way, people would have due notice of possible sharing of information by other agencies or state or local governments.

Thirdly, out of these directives, a graphic national information-flow chart would be designed and make available for public inspection. An individual concerned about his record could then go to the respective agencies and exercise his rights under the Freedom of Information Law to inspect his files.

Fourth, there is a need to fully implement the principle of open government implicit in the Freedom of Information Law by reducing the number of exemptions in it which the Executive Branch may use to deny or withhold information. This would make the judicial remedies it contains more meaningful.

Fifth, I believe there must be established a new independent agency for setting and enforcing strict standards in software and hardware for the assurance of security, confidentiality and privacy of records. These would be applied to all phases of gathering, processing and transmitting information about people by government computer systems. This would include such problems as interception of electronic transmissions and tapping of systems.

Sixth, Congress must enact specific prohibitions on unconstitutional or unwise practices which unfairly augment government's power to invade individual privacy. Examples of such legislation would be: (1) a ban on use of military resources to conduct unwarranted surveillance over civilians and to create and share data banks on them, and (2) a ban on unconstitutional means of coercing citizens into revealing personal information about themselves.[59] Such a bill is S. 2156 which would prohibit requirements on applicants and employees to submit to lie detectors in order to work.[60] Another bill is S. 1438, designed to protect federal employees and applicants from unwarranted demands for information about such matters as their race, national origin, religious beliefs and practices, sexual attitudes and conduct, and personal family relationships.[61] Another necessary protection would be a prohibition on distribution of arrest records to private companies and severe restrictions on their availability within government.[62]

Seventh, is the need for America to take a stand on whether or not every person is to be numbered from cradle to grave, and if so whether or not that number is to be the social security number. Until now, the idea of a universal standard identifier has been merely discussed in philosophical terms, but the need to reduce people to digits for the computer age has prompted wide government use of the number for identifying individuals in government files. Private industries, businesses and organizations have followed suit to the dismay of many people who have registered strong complaints against this practice with the Subcommittee. They were supported by the findings of a Social Security Task Force which reported in 1971 that:

"The increasing universality of the Social Security Number in computer data collection and exchange presents both substantial benefits and potential dangers to society; and that in order to maximize the benefits and minimize the dangers, there needs to be developed a national policy on computer data exchange and personal identification in America, including a consideration of what safeguards are needed to protect individuals' rights of privacy and due process." [63]

In outlining the areas in which state legislatures and the Congress must make important judgments, this Task Force stated:

"Defining the proper role of the Social Security Number in society requires that broad social judgments be made first about the desirability of large-scale computer recordkeeping in various settings; second, about the kinds of data necessary

---

[59] S. 1791, 91st Cong., 1st Sess. (1969).
[60] Senate remarks of Senator Ervin, 117 CONG. REC. (daily ed. June 24, 1971.)
[61] See S. Rep. 92–554 for legislative history (Now pending before the House Post Office and Civil Service Committee with House versions).
[62] 1971 Hearings at 782 (complaints read into the hearing record by the Chairman).
[63] Social Security Number Task Force Report to the Commissioner 17 (May, 1971).

and appropriate to record about individuals within a given setting; third, about the safeguards needed to insure that the computer is being used within a given setting in ways that protect fundamental human rights; and fourth, about the desirability of *any* kind of universal identification system in terms of its psychological impact on the individual citizen." [64]

SUMMARY

From the Subcommittee study of privacy and government data banks one conclusion is undeniable. This is that the extensive use of computerized systems to classify and analyze men's thoughts, speech, attitudes, and lawful First Amendment behavior raises serious questions of denial of substantive due process to our entire society. To try to condense the truth about what men believe and why they believe is a futile exercise which can lead to that tyranny over the mind against which Thomas Jefferson swore eternal hostility. Without grave dangers to our constitutional system, we cannot permit government to reduce the realities of our political life and the healthy traffic in our marketplace of ideas to marks on magnetic tapes and data on a microfilm.

Professor Robert Boguslaw [65] eloquently described the dangers posed by this "technology-screened power" when he wrote that "the specification of future and current system states within this orientation characteristically requires an insistence upon a uniformity of perspective, a standardization of language, and a consensus of values that is characteristic of highly authoritarian social structures. Nonconforming perspectives, language, and values can be and, indeed, must be excluded as system elements."

He further points out certain engineering truths and certain human truths which face every politician, administrator, analyst and programmer who tries to use computers to convey either more or less than the straight facts about people. First is the truth that the strength of high-speed computers is precisely in their capacity to process binary choice data rapidly. But to process these data, the world of reality must at some point in time be reduced to binary form. Second is the truth "that the range of possibilities is ultimately set by the circuitry of the computer, which places finite limits on alternatives for data storage and processing." Third is the truth "that the structure of the language used to communicate with the computer restricts alternatives." Then there is the truth "that the programmer himself, through the specific sets of data he uses in his solution to a programming problem and the specific techniques he uses for his solution, places a final set of restrictions on action alternatives available within a computer-based sytem."

It is in this sense that computer programmers, the designers of computer equipment, and the developers of computer languages possess power in our society.

These limitations of men as well as machines are what I remembered as I listened to the young Army analyst describing his assignment to condense truth for the Army data systems by assigning numbers to people on the basis of their speech and thoughts.[66]

---

[64] Id. at 15.

It is clear that if the SSN became the single number around which all or most of an individual's interactions with society were structured, and if practices of the sort we have been discussing were to continue, the individual's opportunity to control the circumstances under which information about himself is collected and disclosed would be greatly circumscribed.

[65] See Boguslaw, The New Utopians (1965), especially the chapter entitled The Power of Systems and Systems of Power at 181, 186, 190. I would dispute his observation of some years ago that people in the information-processing profession "are scientists and engineers—objective experts whose only concern is technical efficiency and scientific detachment." Id. at 198. It is indeed true, however, that: to the extent that customers (and this may include government agencies or private industry) abdicate their power prerogatives because of ignorance of the details of system operation, de facto system decisions are made by equipment manufacturers or information-processing specialists. Id. at 198.

Implicit in the various issues raised during the Subcommittee Hearings is the wise observation of Professor Boguslaw that:

The paramount issues to be raised in connection with the design of our new computerized utopias are not technological—they are issues of values and the power through which these values become translated into action. Id. at 200.

In this case, I believe it is the constitutional value protected by the First Amendment.

[66] See note 53 supra.

On the shoulders of technology experts who are aware citizens rests the responsibility for guiding those politicians who seek computer-based solutions to political problems. At this point in our history, they, more than anyone, realize that computers have only those values which are designed and programmed into them.

If the attitude of the present Administration is any indication, Government will make increasing use of computer technology in pursuit of its current claim to an inherent power to investigate lawful activities and to label people on the basis of their thoughts. Municipal, state and federal agencies continue to plan, devise and build intelligence systems for many purposes. It devolves on those people involved in computer technology to make known the restrictions and the limitations of the machines as well as the alternatives for what is proposed. When the political managers ignore or abdicate their responsibility to assure the application of due process of law, they may have the final say over the constitutional uses of power.

What they say may not be popular with those who use their services, especially government departments. But I would suggest that when they advise on extending the power of government, they serve a higher law—the Constitution.

The technological forces which affect the quality of our freedoms come in many guises and under strange terminology. They are dreamers who would decry the advent of the computer as casting some sorcerer's shadow across an idlyllic land. In their philosophical rejection or fear of this most intricate of machines, they would deny the spark of divinity which is the genius of man's mind; they would reject the progress of civilization itself. So there is no reason to condemn out of hand every governmental application of computers to the field of information processing or to systems study.

Our society has much to gain from computer technology. To assure against its political misuse, however, we need new laws restricting the power of government and implementing constitutional guarantees. We need increased political awareness of an independent nature by information specialists who understand the machnes and the systems they constitute.

We do not, as some suggest, need new constitutional amendments to deal with these problems. The words of the original amendments will do, because they envelope our national concepts of personal freedom and I believe they can encompass anything which jeopardizes that freedom.

As Justice Oliver Wendell Holmes said:

"A word is not a crystal, transparent and unchanged; it is the skin of a living thought and may vary greatly in color and content according to the circumstances and the time in which it is used." [67]

I believe that Americans will have to work harder than ever before in our history so that the First Amendment remains a living thought in this computer age.

Otherwise, we may find the individual in our society represented not by a binary form, but by one digit.

And that will be "zero."

Otherwise, America may lose its cherished reputation as "the land of the Second Chance."

---

[67] Towne v. Eisner, 245 U.S. 418, 425 (1918).

[EXCERPTS FROM THE UNIVERSITY OF ILLINOIS LAW FORUM, VOL. 1971, NO. 2]

Copyright 1972 by the Board of Trustees of the University of Illinois

PRIVACY AND GOVERNMENT INVESTIGATIONS†

*Senator Sam J. Ervin, Jr.**

SINCE THE DAWN of civil society, men have contended over the ways government exercises its investigative power as they have contended over the ways to reach heaven. Americans in the twentieth century offer no exception to this truth. Their concern is the greater because privacy is valued in our society as a hallmark of freedom. Yet recently it has been threatened or diminished in ways and for reasons that to some people seem beyond our challenge or our control.

There are those in our country who believe that to enforce the laws, government should investigate everything and there are those who believe that to preserve liberty, government should investigate nothing. There are those, and I count myself among them, who believe that government must have ample power to investigate and to gather information in order to govern, but who also believe that there are certain things which are none of the business of government. There are those, and I count myself among them, who believe that a free society must take some risks in order to remain free, but who also believe that, similarly, the individual under a government of laws must assume the risks and the legal consequences for his actions.

The glory of our constitutional system is that its authors set down for the ages the lessons learned about man's struggle to control governmental power. As we discuss the power of government to investigate and to monitor the activities of those it governs, we have ever before us certain fundamental principles governing the exercise and control of power over the individual in our society. It is those constitutional principles, designed to keep all men free in their minds and in their spirits, which I believe will see America through any crisis. If these principles are meticulously observed, I believe neither wars nor natural disasters, neither threats from beyond our borders nor threats from within, neither dissent nor rebellion, neither economic perils nor political instability will founder this nation.

In the crisis atmosphere in which government officials must frequently operate as they attempt to solve major social and economic

† *These remarks were originally delivered as a lecture in the Privacy and the Law Series at the University of Illinois College of Law, May 7, 1971.*

**United States Senator from North Carolina. B.A. 1917, University of North Carolina; LL.B. 1922, LL.D. 1951, Harvard University; LL.D. 1955, Western Carolina College.*

problems, there are some forces at work which often make it difficult to assure the proper balance between the needs of government and the freedom of the individual guaranteed by the Constitution. I want to stress that while we should be on guard against the adverse effects of these forces, I think that properly channeled, they may be counted among America's best hopes for creative progress.

One of these forces is the increasing demands on government for new and better services of all kinds. Another is the greater political awareness and activity on the part of citizens from every walk of life who want to have greater influence on their government and a larger role in helping to shape policy.

Another force is computer technology and the use of scientific methods of systems analysis which it encourages. In a study by the Constitutional Rights Subcommittee, we found that the increased use of government and private computer-based systems is making it vastly more economical to acquire and store information about people for reasons which should give Americans serious pause. It is creating not only an army of specialists in the information-processing field, but battalions of investigators and analysts specializing in seeking out and reporting derogatory information on individuals.[1] It is feeding the zeal of statistics collectors in government who claim they need information for research and who back their requests for data with the sanctions of criminal and civil law.[2]

There is another force affecting our privacy caused by the development of the behavioral sciences with their emphasis on analysis of man's behavior in society and organizations, their emphasis on what makes him think as he does and act as he does, and on what elements go to make up his personality. This wave of personality study has taken over government and private industry alike. In its name, many sophisticated questionnaires and pseudoscientific instruments such as personality tests and lie detectors have been developed to elicit personal information.[3]

The result of all this is that officials at every level of our national life who make decisions about people for limited purposes seem possessed by a desire to know the "total man" by gathering every possible

1. *See* Ervin, *The Computer and Individual Privacy*, 113 CONG. REC. 5898 (1967) (address before the American Management Association, on March 6, 1967); *see also* comments by Senator Ervin on computer abuses and suggested remedies, 115 *id.* 33576, 39114 (1969).

2. *See generally Hearings on S. 1791 and Privacy, the Census and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm.*, 91st Cong., 1st Sess. (1969). Ervin, *Privacy, the Census and Federal Questionnaires*, 115 CONG. REC. 17718 (1969).

3. *See Hearings on Psychological Tests and Constitutional Rights Before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm.* (1965); Remarks of Senator Ervin on S. 2156, A Bill To Protect Against Invasion of Privacy by Prohibiting Lie Detectors, 117 CONG. REC. S. 9870 (daily ed. June 24, 1971).

bit of information about him. The further result is that government and private computers and dossiers are filled to overflowing with the trivia of the daily lives of people. Although frequently meaningless, the trivia obtain in official reports of government agencies and credit companies an infallibility which can adversely affect a person's life and fortunes, and even his honor.[4]

Yet all of these forces are at work on agencies and organizations operating under laws meant, for the most part, for another era, less oriented to the need for total information and less in need of rapid analysis and cross-country transmission of data.

There have been many charges recently of illegal privacy invasion, especially about the surveillance practices of the Federal Bureau of Investigation. Many people equate the activities of that agency with those of the Army, whose broad program for data-gathering on civilian politics has been widely criticized and discussed recently. I believe they fail to realize the differences. The FBI, it is true, has very broad investigative powers, and along with other agencies its investigative reports frequently contain nothing but trivia. Its methods, along with those of other agencies, may need some ethical refurbishing. On the other hand, it is sometimes forgotten that, unlike the Army, the Bureau has been given legal responsibilities for investigating a great range of federal criminal laws, many of them vaguely worded. These include all of our espionage and security laws. They include the broad investigations demanded by the 1954 executive order which President Eisenhower issued requiring the FBI, the Civil Service Commission, and other agencies to investigate an individual's character, morals, emotional stability, and good judgment in order to determine if he might become a security risk.[5] So, if some are finding that in our computer age the investigative power of federal law enforcement officers should perhaps be better defined in writing, that is not necessarily the same as saying that the officers have been acting illegally.

. . While there may be misunderstanding on the part of some about the FBI, I do not agree with those who claim it is "political demagoguery" and "hysteria" to speak of violations of privacy and constitutional rights by government investigations. Indeed, I believe it is timely to do so if our fundamental freedoms are to be preserved.

I say this because it is clear to me from the complaints coming to Congress that the combination of executive branch politics and these

4. A.R. MILLER, THE ASSAULT ON PRIVACY 67-89 (1971); *Hearings on S. 823 and Fair Credit Reporting Before the Subcomm. on Financial Institutions of the Senate Comm. on Banking and Currency*, 91st Cong., 1st Sess. (1969); *Hearings on H.R. 16340 and Fair Credit Reporting Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency* (1970).

5. *Security Requirements for Government Employment*, Exec. Order No. 10,450, 3 C.F.R. 936 (1953), *as amended*, Exec. Order No. 10,550, 3 C.F.R. 200 (1954).

three social forces I have described has produced a novel claim in the executive branch to an inherent constitutional power to investigate people whose only crime is exercise of their first amendment freedoms.

This claim of investigative power is founded in the desire to predict violations of the law and to take preventive measures before there is any overt sign of intent to commit a crime. It is founded in a very human curiosity to know what people are thinking. The problem is that it clashes with the fundamental constitutional principle that what people are thinking is none of the business of government investigators. I believe that, unchecked, the exercise of such an inherent power can quickly give this nation the trappings of a police state.

The Subcommittee has discovered a number of instances of agencies who started out with a worthy purpose for investigating, but who, under the inherent power concept, went so far beyond what was needed in the way of information that the individual's privacy and right to due process of law are threatened by the very existence of the files the agencies collected.[6]

One massive investigative program pursued under this inherent power theory was the Army's civil disturbance prediction program which caused it to spy on thousands of Americans in order to try to predict when disturbances would occur which could not be controlled by local or state police power and when the President would be requested to supply military assistance.[7]

Concern about Army prying into civilian affairs has been expressed to Congress by people in every state of the Union. There has been special concern in Illinois because of the publicity given the surveillance activities of the 113th Military Intelligence agents.

It is the students of the law who because of their special knowledge of the Constitution can perhaps best understand the threats to liberty caused by the kind of Army surveillance, investigation, and data collection described recently before the Senate Constitutional Rights Subcommittee.[8]

I think it should be stated here that despite their failings, Army officials were not the chief focus of our investigation. For a number of years, the Subcommittee has received many complaints about excessive

6. *See generally* Remarks by Senator Ervin announcing hearings on computers and data banks and describing responses to Subcommittee survey of federal departments and agencies, 116 CONG. REC. 30797 (1970), 117 *id.* S. 985 (daily ed. Feb. 8, 1971).

7. For an account of developments in this investigation of the Army surveillance and data banks, together with relevant articles and texts of correspondence *see generally* 116 CONG. REC. 2225, 5496, 26327, 41751, 43944 (1970) (Remarks of Senator Ervin).

8. Pyle, *Conus Intelligence: The Army Watches Civilian Politics*, Washington Monthly, Jan. 1970; Pyle, *Conus Revisited, id.* July 1970. These articles also appear with remarks by Senator Ervin, 116 CONG. REC. 2225, 5496 (1970).

federal demands for personal information from people, about haphazard computerization, exchange and distribution of data without proper safeguards, and about data banks for storage of all kinds of extraneous information unrelated to the needs of the agency.

We initiated a survey of all departments to learn what laws and rules govern these data banks and computers and how they affect the privacy of the individual. One of our original reasons, therefore, for investigating the Army was to learn what computers and data banks the Department of Defense maintained on people. The Subcommittee has experienced considerable difficulty with many departments in obtaining frank answers to our inquiries, but the Army, it is safe to say, has been the least frank of all.

During our hearings on computers, data banks, and the Bill of Rights,[9] we learned that the Army has been assigned the work of a national police force. It had been given the task of spying upon American citizens who were exercising their first amendment freedoms. In pursuance of this mission, the Army technocrats put into use an arsenal of surveillance weapons and techniques. These included the products of personal observation of agents, as well as computers, microfilm data banks, video recorders, photographs, card files, and manual files.

Such a program was fraught with danger for the very freedoms which were designed to make the minds and spirits of all Americans free and which work to keep America a free society. It is those first amendment freedoms which are the most precious rights conferred upon us: the freedom to think one's own thoughts regardless of whether they are pleasing to government or not; the freedom to speak what one believes whether his speech is pleasing to the government or not; the freedom to associate with others of like mind to further ideas or policies which one believes beneficial to our country, whether such association is pleasing to government or not; the freedom to assemble peaceably with others and petition government for a redress of grievances; and the freedom to worship Almighty God according to the dictates of one's own conscience.

Notwithstanding these freedoms conferred by the Constitution, the Army spied upon people attending divine services in churches; it infiltrated religious organizations; and it placed large groups of Americans under surveillance when the only offense committed was to exercise their first amendment freedoms.

On one occasion 119 persons met together to protest certain poli-

9. See generally *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm.*, 92d Cong., 1st Sess. (1971) [hereinafter cited as *1971 Hearings*]. Prepared statements of witnesses who testified on the Army program are also collected in *Uncle Sam Is Watching You: Highlights from the Hearings of the Senate Subcommittee on Constitutional Rights*, Public Affairs Press (1971).

cies of government with which they disagreed. Their meeting was entirely peaceable and nonviolent. Yet it turned out that only sixty-seven persons were protestors and that a very large number were military and law enforcement agents ordered, along with the press, to attend this meeting, to take pictures of the persons present, and to tape the speeches which were made. One military intelligence agent in attendance said that the speeches were wholly nonviolent in nature but that they could not tape them because of the noise of five Army helicopters which flew directly over the meeting during its continuance, spying upon the 119 people from above.[10]

The Subcommittee was told that with very little in the way of guidelines for their activities, the Army maintained computerized microfilm and manual files on membership, ideology, programs, and practices of virtually every activist political group in the country.[11]

These included not only violence-prone organizations, but also such nonviolent groups as the American Friends Service Committee, the Southern Christian Leadership Conference, Clergy and Laymen on the War in Vietnam, the American Civil Liberties Union, the Women's Fight for Peace, and the National Association for the Advancement of Colored People. Groups as diverse as the Ku Klux Klan, the Communist Party, the Students for Democratic Society, and Businessmen Against Vietnam were covered. Intelligence agents testified that they were ordered to infiltrate groups protesting various government policies.[12] They joined peace groups, monitored mothers' meetings, attended community poverty board meetings, and reported on campus events, activities, and classes.

Now the military did not just collect all of this information and keep it secret. The Army shared their blacklists with many federal, state, and local agencies.[13] They had their analysts study the data and try to codify it in order to put it into computers and microfilm data banks. One intelligence analyst told the Subcommittee how the Counter Intelligence Analysis Branch received reports on persons often obtained covertly by Army agents and FBI informants. These reports contained detailed information on finances, sexual activities, personal beliefs, and associations of famous people, as well as anonymous Americans. They contained detailed background investigations on anti-war protestors arrested by local police for misdemeanor offenses, as well as

10. *1971 Hearings* 315 (testimony of Laurence Lane).
11. *Id.* 147 (testimony of Christopher N. Pyle).
12. *Id.* at 244.
13. For a list of the federal agencies requested to furnish information to the Army see Appendix B to the *Department of the Army Civil Disturbance Information Collection Plan of May 1968, 1971 Hearings* pt. 2. The text also appears in 117 CONG. REC. S. 2290 (daily ed. March 2, 1971) (remarks of Senator Bayh). For the Army distribution list for its own data and the number of copies each agency received see Appendix D to the *Information Collection Plan, supra.*

reports on speeches in all of our cities.

To make the difficult decisions about what category a person belonged in, the analyst was required to examine these reports and then resort to a special intelligence code. He had to apply various number combinations which indicated a person's beliefs or status. For instance, 134.295 indicated that a person was a non-Communist, while 135.295—a difference of one digit—indicated Communist Party membership or advocacy of Communism. We were told that since many of these persons were young people with no political philosophy and no organized memberships, the analyst had nothing to go on but some political utterances. On the basis of these, he sometimes chose a designation arbitrarily in doubtful cases.[14]

Despite all of the information-gathering, the computers, and the data banking, the Subcommittee has yet to be told why this was thought to be useful. I found no instance when a doughboy sniped on in Detroit would have found this information useful. In fact, the Deputy Chief of Staff of the Army Intelligence Command didn't even know there was a computer program at Fort Holabird. The Subcommittee was first told informally that there were no computers; then, that there was one, but that it had been disconnected for this program; then, that there were a few more computers that the Defense Department had forgotten about or not known about.

On the basis of all the confusion displayed by these officials, it became clear to me that computers have far too much privacy in the Army as well as elsewhere in the executive branch.

The Subcommittee has been unable so far to discover exactly who ordered this surveillance, how useful the information was, how extensive the program was, and how many churches, universities, and communities were spied on. The Department of Defense in their testimony admitted little more than we had been told by the press, former agents, and other sources. This is despite our continuous requests for pertinent documents and for the testimony of the generals and officers with most knowledge about the program.[15]

I do not, however, believe the Army proceeded on its course alone or unauthorized. Someone tried to make prophets out of some G.I.s serving out their tour of military duty.

The Army was finally given a Civil Disturbance Plan to follow for

14. *1971 Hearings* 248, 260 (Stein testimony).

15. For an account of the Subcommittee requests for testimony of knowledgeable civilian and military officials, for declassification of pertinent documents and delivery of others *see generally* the exchange of correspondence between Senator Ervin and Defense Department officials between July 29, 1970 and Dec. 4, 1971, *1971 Hearings* pt. 2 (App.). For a discussion of the constitutional issues and a list of the Defense Department's reasons for their withholdings and delays see Ervin, *Secrecy in a Free Society*, 213 NATION 454 (1971).

its activities in January 1968.[16] They were told to watch people in the civil rights movement, the anti-draft movement, and in labor disputes. This "Plan" was supplemented in February 1968 by a document setting forth the intelligence interest of the Army.[17] It shows that all this information was to be collected despite the recognition that the majority of civilians were law abiding. The "Intelligence Annex (B)" said that "although the majority of anti-war protestors appear reluctant, for moral, practical, or legal reasons, to engage in public demonstrations of a nature which violates existing laws, there is a significant minority of professional agitators and young students who advocate either violent action or so-called disobedience." Then the Plan said that, while it recognized that the majority of the people who participate in these activities were loyal Americans, there was an apprehension that they might be under the direction of some foreign groups and might not know their own minds. It stated that notwithstanding the fact that most of the black population abhors violence, these people might still be made dangerous to society by the militants.

Another document supplementing the January Plan was the Civil Disturbance Information Collection Plan of May 1968, which shows that the Army agents and commanders were to gather information about "threshold activity" and pre-civil disturbance matters. Other federal law agencies and military departments were asked to supply similar information. They were told to find out "the identity of newspapers, radio or television stations, and the names of prominent persons friendly with the leaders of the disturbance and who were sympathetic to their plans. Whether any would be present, participating, and how." They were told to find out the probable categories and identification of persons and groups who would create or participate in a civil disturbance, the estimated number of persons who would be involved as participants and as observers, and the overt and behind the scenes leaders' identity. The Army wanted to know about protests of the minority community to conditions in slum areas such as de facto segregation in unions, housing, and schools, and such as local merchants and landlords overcharging for housing and goods. They wanted to know about efforts by minority groups to upset the balance of power and the political system.

They asked about the "high command" of dissident groups, their organizational charts, rosters of key personnel, and the numbers of active members; the breakdown of membership by ethnic group, age, economic status, education, criminal record, and biographic data on key members.

16. *1971 Hearings* 398, 419. As of Dec. 1971, neither the basic Jan. 1968 Plan nor the Army's new 1970 Civil Disturbance Plan had been declassified.

17. *1971 Hearings* pt. 2 (App.). Annex B (Intelligence) to Dept. of the Army Civil Disturbance Plan (Feb. 1, 1968, unpublished).

They wanted information on "evidence of or attempts by subversive organizations to penetrate and control civil rights or military organizations composed primarily of non-whites."

They wanted to know the "aims and activities of groups attempting to create, prolong, or aggravate racial tensions, such as CORE, NAACP, SNCC, National States Rights Party, Southern Christian Leadership Conference, and the Council of Federated Organizations." As a separate category, they even wanted information about the women members of such groups.

With such a broad mandate, it is small wonder that zealous commanders and industrious agents felt that they had to scoop up everything of possible interest in their reports and that they would feel required to keep under surveillance every politically active citizen and group exercising first amendment freedoms.[18]

I asked the Assistant Secretary of Defense, Mr. Froehlke, if he thought that existence of this information system would not have a debilitating effect upon the exercise of the constitutional rights of free speech and assembly by many of our politically aware citizens. He replied that he didn't think there was any violation of the first amendment.[19]

"We maintain there was no illegal activity. We think we maintain there was inappropriate activity," he said. He admitted that some of the Army's activities didn't "make much sense" from the management point of view, but he didn't know whether he would call them "illegal."[20] Merely watching someone, he testified, does not violate any constitutional rights, unless there was some "specific evidence that someone was deterred." If it was unknown, it was argued, the man wouldn't know it, so it could hardly deter his activities. Of course, it must be noted that the Army did more than "watch." They took notes, made dossiers, photographed, and tape recorded.

In my opinion, the argument that blacklists and surveillance programs which are unknown to the public can't hurt anyone is specious. Such an argument is common in government, but it flies in the face of the principle of open government which is the keystone of our Constitution. It denies the basic right of the people to full information about the activities and programs of their government. This is the constitu-

18. *1971 Hearings* 421, 422 (testimony of Assistant Secretary of Defense Robert F. Froehlke).

19. *Id.* at 430.

20. *Id.* 431. See also *id.* at 385 (Froehlke testimony):

> It is worthy of note that none of the activities referred to above were prohibited by Federal or State law . . . . Since no use of civil disturbance information was made or intended to be made that would result in any action to the prejudice of any individual or organization, it is difficult to perceive how the constitutional rights or even the right of privacy could be impinged by the collection of such information.

63-619 O - 76 - 81

tional principle which was implemented recently in the Freedom of Information Act[21] and which is reflected in many other statutes requiring disclosure and full reports of government programs. The Froehlke argument assumes that people will not find out about illegal or unconstitutional programs. If Mr. Froehlke needed more proof that unconstitutional programs cannot be hidden from the people for very long, he has only to look at the history of the Army's civil disturbance program and he has only to consider the shock and dismay of the American people which they expressed to Congress as the full scope of this program was made known to them by former agents and by the press.

Some executive branch officials have not yet discovered the truth of Abraham Lincoln's observation, for it is clear from their arguments on this matter that they think the government can fool all the people all of the time. Secretary of Defense Laird and the Army sent word that the intelligence-gathering on civilians was being cut back and that the computers, in effect, were unplugged. He said the Army would henceforth rely on the Department of Justice for civil disturbance information.[22]

In view of that assertion, I asked the Attorney General, as chief legal officer of the Government, for his opinion on the constitutionality of the collection of information by the Army or other executive departments on people who were not suspected of breaking any laws but who were merely exercising their first amendment rights.[23]

He delegated this task to the Assistant Attorney General, Mr. Rehnquist, who told the Subcommittee that he didn't think it would stifle first amendment freedoms to place such persons under surveillance.[24] He said that "[i]t may have a collateral effect such as that but certainly during the time the Army was doing things of this nature, and apparently it was fairly generally known that it was doing these things, it didn't prevent two hundred fifty thousand people from coming to Washington on at least one or two occasions to protest the war policies of the President."

He also told us that while there might be " 'isolated abuses' of the investigative function, they were not unconstitutional."[25]

He further stated that he knew of no authoritative decision holding that it was unconstitutional to collect information which is not le-

21. 5 U.S.C. § 552 (1970).

22. *1971 Hearings* 394. *But cf. id.* at 436 (Froehlke testimony): "Nevertheless, experience has taught me that I cannot tell you that under no circumstances should the Army ever observe non-DOD-affiliated civilians. I think under certain extreme circumstances the Army might again have to, and that is the criteria we are talking about."

23. *Id.* at 571. The Subcommittee letter to the Attorney General also appears with remarks by Senator Ervin, 116 CONG. REC. 26327 (1970).

24. *1971 Hearings* 620.

25. *Id.* at 602, 603.

gitimately related to the statutory or constitutional authority of the executive branch to enforce the laws.[26] It was his contention that there is no constitutional rights violation by government investigation and data-gathering unless a government sanction is involved.[27] My own suspicion of an unchecked executive branch investigative power was borne out during his testimony when he advanced the amazing theory that "self-discipline on the part of the executive branch will provide an answer to virtually all of the legitimate complaints against excesses of information-gathering."[28]

Mr. Rehnquist and other Justice Department officials bandied about a vague theory of preventive law enforcement which justifies surveillance.[29] They cited article III, section 3 of the Constitution as the "source of the duty of the President to oversee the faithful execution of the laws and thereby exercise implicit power to investigate, prosecute, and prevent violation of the Federal law." As another source of information-gathering in the executive branch, they cited article IV, section 4, providing that the United States shall guarantee every state a "Republican Form of Government," and on application of the legislature, or of the executive, [shall protect each] "against domestic Violence."[30] They cited an 80-year old Supreme Court decision, *In re Neagle*,[31] involving a shoot-out between two judges. They cited statutes on the federal role in civil disturbances.[32] But they conveniently ignored the Bill of Rights.

Rather, they, like the Army, laid claim to a constitutional power of investigation for purposes of preventive law enforcement which, given the scope of federal criminal and civil laws, if carried to its logical extremes, could justify surveillance of any citizen for almost any purpose whatsoever.

26. *Id.* at 602.
27. *Id.* at 620.
28. *Id.* at 603.
29. *Id.* at 602.
30. *Id.* at 599.
31. *In re Neagle*, 135 U.S. 1, 10 S. Ct. 658 (1890).
32. 10 U.S.C. §§ 331-33 (1970). Under U.S. CONST. art. 1, § 4, and 10 U.S.C. §§ 331-33 (1970), the President has authority to use the armed forces for these purposes:

1. To suppress rebellion, insurrection, or domestic violence, which obstructs the execution of the laws of the United States, or impedes the course of justice under those laws.
2. To suppress insurrection against a state if state authorities so request.
3. To suppress insurrection or domestic violence in a state, which so hinders the execution of federal or state laws within the state as to deprive "any part or class of its people . . . of a right named in the Constitution and secured by law" if the constitutional authorities of the state (a) are unable, (b) fail, or (c) refuse to protect that right.

10 U.S.C. § 334 (1970) provides that whenever the President considers it necessary to use the armed forces under §§ 331-33, "he shall, by proclamation, immediately order the insurgents to disperse and retire peaceably to their abodes within a limited time."

I must take issue with the Department of Justice officials on all of these counts, for I believe they fail to understand the relationship between constitutional liberty and the government's claim to a power to investigate people in order to determine future behavior.

First, contrary to the opinion offered by the Assistant Attorney General, recent events have shown that there is indeed a need for strict legislation in this area of the law. "Self-discipline" is not enough. It has not prevented the Army spying on civilians; it has not precluded the Census Bureau and other information-gathering agencies from harassing people with broad questionnaires. It has not prevented the continuing inquiries into the most private lives and beliefs of federal employees and applicants. It did not stop the Secret Service from computerizing people who write letters about their grievances to high government officials, who are professional gate-crashers, and who make remarks embarrassing to high government officials at home or abroad. "Self-discipline" does not help the wives of applicants for FHA loans when they are compelled to disclose their birth control practices and confidential advice from their doctors. Nor has "self-discipline" prevented all the other programs from violating personal privacy.

So I believe there must be new laws geared to the computer age, with specific guidelines for gathering personal data and with carefully drawn controls on the use, exchange, and protection of such information. Furthermore, I believe that some provision must be made to provide the individual access to government records about him and the chance to assure the accuracy of such information.[33]

Secondly, contrary to the opinion of lawyers at the Justice Department, I have found that the courts have long been active in this area, and I predict that they will be even more active if the executive branch continues to try to make prophets of its civil servants and if it continues in its present claim to an inherent power to make inquiries in the course of trying to predict the future behavior, attitudes, and beliefs of law-abiding Americans. For instance, the United States Supreme Court will soon consider the case of *Laird v. Tatum,*[34] a suit challenging the

33. For an excellent discussion of the constitutional, legal, and philosophical problems involved in such an effort for one area of information-gathering *see generally Security and Privacy Considerations in Criminal History Information Systems,* Technical Rep. No. 2, July 1970, by Project SEARCH, California Crime Technological Research Foundation, funded by the Law Enforcement Assistance Administration, Department of Justice. Related to this issue is S. 2546, A Bill To Facilitate and Regulate the Exchange of Criminal Justice Information Systems, introduced by Senator Roman Hruska Sept. 20, 1971. 117 CONG. REC. 14563 (daily ed. Sept. 20, 1971). Also pertinent is the testimony of Richard Velde of the Law Enforcement Assistance Administration on the use of information and intelligence systems by criminal justice agencies. *1971 Hearings* 605, 849, and testimony of FBI officials concerning the National Crime Information Center. *Id.* 914.

34. 444 F.2d 947 (D.C. Cir. 1971), *cert. granted,* No. 71-288, 1971 Term (40 U.S.L.W. 3238).

Army program. Dismissed by the district court as not presenting constitutional rights issues, the case is defended by the Government with the claim that the threat of surveillance is not sufficient to invoke the judicial process and, furthermore, that the plaintiffs have not demonstrated a personal stake in the outcome of the controversy. According to the Justice Department, the record "presents only abstract legal issues involving, at best, the speculative impairment of constitutional rights."[35]

Many people, like the Assistant Attorney General, seem to think this is new legal ground which must be pioneered. These officials have overlooked the significance of numerous court decisions bearing on privacy and the investigative power of government.

On the basis of my study of the decisions, I believe this case law was correctly summarized by Professor Bernard Schwartz in terms which should be brought to the attention of all government agencies. He writes:

> Of course, government may deal at any time with threats to its security expressed in acts. Where speech, association and other First Amendment rights are involved, on the other hand, the power of investigation should be no more far-reaching than that of legislation. In our system, authority over a subject matter involving speech, press, assembly, and the like must not go beyond the power to do that which is essential to be done in protection against a public danger. Civil liberties may not be abridged by investigatory authority merely in order to determine whether they should be abridged.[36]

From reports received by the Constitutional Rights Subcommittee, I think not only the Army investigators, but other federal and local agents are too often engaged in investigations of people merely to determine if they should be investigated or if dossiers should be kept on them. Under Professor Schwartz's test, such practices, wherever they occur, violate first amendment rights.

Thirdly, unlike Administration officials, I think there are serious constitutional rights violations in these surveillance programs.

I have found three Supreme Court decisions in particular which provide a point of departure for courts and legislatures seeking guidance in setting controls on unwarranted information-gathering and data banking. I recommend these decisions to officials in the executive branch who assert a broad claim to investigative power.

The first case is *United States v. Rumely,* decided in 1953.[37] In that case, the accused was the secretary of an organization which, among other things, engaged in the sale of books of a political nature.

35. *Id.* Petitioner's Brief for Certiorari at 10 n.4.

36. B. SCHWARTZ, 1 COMMENTARY ON THE CONSTITUTION OF THE UNITED STATES: POWERS OF GOVERNMENT 140 (1963).

37. 345 U.S. 41, 73 S. St. 543 (1953).

The House Select Committee on Lobbying had called on him to disclose the names of those who made bulk purchases of those books for further distribution. He refused to furnish the names and was convicted under a statute providing penalties for refusing to give testimony or to produce relevant papers upon any matter under congressional inquiry. The Committee claimed authority to demand this under the power, stated in their resolution, to investigate all lobbying activities intended to influence, encourage, or promote legislation.

Justice Frankfurter delivered the opinion of the Court, holding that the accused was not required to deliver the names on the ground that the authorizing resolution restricted the Committee to a study of lobbying activities which were carried on directly with members of Congress and could not extend to a person's effort to influence legislation through the means of books and periodicals. With this as an alternative ground for decision, the Court did not have to reach the constitutional issue. However, the Justice made the significant observation: "Surely it cannot be denied that giving the scope to the resolution for which the Government contends, that is, deriving from it the power to inquire into all efforts of private individuals to influence public opinion through books and periodicals, however remote the radiations of influence which they may exert upon the ultimate legislative process, raises doubts of constitutionality in view of the prohibition of the First Amendment."[38]

Justice Douglas wrote a concurring opinion in which he said that he was compelled to face the constitutional issue that this involved the grant of power to the Committee. He pointed out, in an able opinion with which I thoroughly agree, that the resolution did not give the Committee the power it claimed but that it was unconstitutional as a violation of the first amendment guarantee of the freedom of press and speech. He recognized that no legal sanction was involved here but felt that it could be the beginning of surveillance of the press. Under such a rule, he noted, the spectre of a government agent will look over the shoulder of everyone who reads, and the subtle imponderable pressures of the orthodox will lay hold. "Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press. Congress could not do this by law. The power of investigation is also limited. Inquiry into personal and private affairs is precluded. . . . And so is any matter in respect to which no valid legislation could be had."[39]

Therefore, since Congress could not by law require of Rumely what the House demanded, it could not take the first step in an inquiry ending in fine or imprisonment.

38. *Id.* at 46, 73 S. Ct. at 546.
39. *Id.* at 58, 73 S. Ct. at 551-52 (citations omitted).

The second opinion which I think is very illuminating on this subject is the case of *NAACP v. Alabama*.[40] There the question was presented whether Alabama, consistent with the due process clause of the fourteenth amendment, could compel the petitioners to reveal to the state's attorney general the names and addresses of all of its Alabama members and "agents" without regard to their positions or functions in the Association. Justice Harlan wrote the unanimous opinion of the Court, holding that Alabama was precluded by the due process clause of the fourteenth amendment, which, of course, made the first amendment applicable to the states, from requiring this information. He said, and I commend this to the Department of Justice: "It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."[41]

The Justice noted that inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs. The Court held that the immunity from state scrutiny of membership lists which the Association claimed was so related to the right of the members to pursue their lawful private interest and to associate freely with others in so doing as to come within the protection of the fourteenth amendment. It held that Alabama had failed to make a showing of overriding valid interest in possession of such information and that judgment of the Alabama court punishing the respondent for contempt of court was invalid under the Constitution.[42] It is a natural extension of these decisions to say that, for example, the federal government can't go out and observe people exercising their first amendment rights and then take steps which have the effect of stifling their willingness to continue in the exercise of their first amendment rights.

What inquiries and investigations Congress and the states may not undertake under the Constitution, certainly the executive branch has no inherent power to undertake.

There is another opinion which I think sums up the constitutional law in this field very well. This is the dissenting opinion of Justice Harlan, joined by Justices Frankfurter, Clark, and Whittaker, in the case of *Shelton v. Tucker*.[43] It is in harmony with the *Rumely* and *NAACP* cases, although it differs on conclusions of fact. In the *Shelton* case, the State of Arkansas required every teacher, as a condition of employment or continued employment, to answer a questionnaire requiring among

40. 357 U.S. 449, 78 S. Ct. 1163 (1958).
41. *Id.* at 460, 78 S. Ct. at 1171.
42. *Id.* at 466, 78 S. Ct. at 1174.
43. 364 U.S. 479, 81 S. Ct. 247 (1960).

CHAPTER IV

Selected Bibliography on the Rights of Privacy and Maintenance of Federal Records

The Library of Congress
Congressional Research Service
Washington, D.C. 20540

SELECTED BIBLIOGRAPHY

I. Conceptual Development of Privacy

Bloustein, Edward J. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. New York University Law Review, v. 39, Dec. 1964: 962-1007.

Breckenridge, Adam C. The right to privacy. Lincoln, University of Nebraska Press, 1970. 155 p.

Columbia human rights law review. Winter 1973: entire volume. Articles include: Arthur R. Miller, "Computers, Data Banks and Individual Privacy: An Overview," Sam J. Ervin, Jr., "The First Amendment: A Living Thought in the Computer Age," Nicholas deB. Katzenbach and Richard W. Tomc,"Crime Data Centers: The Use of Computers in Crime Detection and Prevention," Frank Askin, "Surveillance: The Social Science Perspective," Michael A. Baker, "Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern," John P. Flannery, "Commercial Information Brokers."

Davis, Frederick. What Do We Mean by "Right to Privacy"? South Dakota Law Review, v. 4, Spring 1959: 1-24.

Fried, Charles. "Privacy." The Yale law journal, 77 January, 1968: 475-93.

Greenawalt, Kent. Legal protections of privacy. Washington, Office of Telecommunications Policy [1975] 130 p.

_____. Privacy and its legal protections. Hastings Center studies, v. 2, Sept. 1974: 45-68.

Henkin, Louis. Privacy and Autonomy. Columbia Law Review, v. 74, Dec. 1974: 1410-1433.

Law and contemporary problems. v. 31, Spring 1966: entire volume. Articles include: William M. Beaney, "The Right to Privacy and American Law;" Milton R. Konvitz, "Privacy and the Law: A Philosophical Prelude;" Edward Shils, "Privacy: Its Constitution and Vicissitudes;" Sidney M. Jourard, "Some Psychological Aspects of Privacy;" Harry Kalven, Jr., "Privacy in Tort Law--Were Warren and Brande is Wrong?"; Kenneth L. Karst, "'The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data," Joel F. Handler and Margaret K. Rosenheim, "Privacy in Welfare: Public Assistance and Juvenile Justice," and William A. Creech, "The Privacy of Government Employees."

Lusky, Louis. Invasion of Privacy: A clarification of concepts. Political science quarterly, v. 77: 2 June 1972: 192-209.

Miller, Arthur R. The assault on privacy: computers, data banks, and dossiers. Ann Arbor, The University of Michigan Press, 1971.
One of the best sources on privacy and the computer.

Parker, Richard B. A Definition of Privacy. Rutgers Law Review, v. 27, 1974: 275-296.

Pennock, J. Roland and John W. Chapman, ed. Privacy. Nomos XIII: Yearbook of the American Society for political and Legal Philosophy. New York, Atherton Press, 1971. 255 p.

Rule, James B. Private Lives and Public Surveillance: Social Control in the Computer Age. New York, Schocken Books, Inc., 1974. 382 p.

Thomson, Judith Jarvis. The right to privacy. Philosophy and public affairs, v. 4, summer 1975: 295-314.

Warren, Samuel D., and Louis D. Brandeis. The right to privacy. Harvard law review, v. 4, December 1890: 193-220

Westin, Alan F. Privacy and Freedom. New York, Atheneum Press, 1967. 487 p.

II. Privacy Act of 1974

Association of the Bar of the City of New York. Committee on Federal Legislation. Government data banks and privacy of individuals (H.R. 16373 and S. 3418). Record of the Association of the Bar of the City of New York, v. 30, Jan.-Feb. 1975: 55-106.

Bigelow, Robert P. The Privacy Act of 1974. Practical lawyer, v. 6, Sept. 1975: 15-24.

Cohen, Richard E. Agencies prepare regulations for implementing new privacy law. National journal reports, v. 7, May 24, 1975: 774-777.

Goldstein, Robert C. The costs of privacy. Datamation, v. 21, Oct. 1975: 65-69.

Government information and the rights of citizens. Michigan law review, v. 73, May-June 1975: whole issue.

Hanus, Jerome J. A Right of Information Privacy. Journal of Policy Studies, v. 4, winter 1975: 136-141.

U.S. Congress. House. Committee on Government Operations. Subcommittee on Foreign Operations and Government Information.
Access to records. Hearings, 93d Congress, 2d session on H.R. 12206 and related bills. Washington, U. S. Govt. Print. Off., 1974. 338 p.

U.S. Congress. Senate. Committee on Government Operations and Committee on the Judiciary. Ad Hoc Subcommittee on Privacy and Information Systems and the Subcommittee on Constitutional Rights. Privacy: the collection, use, and computerization of personal data. Joint hearings, 93d Congress, 2d session, on S. 3418, S. 3633, S. 3116, S. 2810, and S. 2542. 2 v. June 18, 19, and 20, 1974. Washington, U.S. Govt. Print. Off., 1974. 2335 p.

U.S. National Bureau of Standards. Computer security guidelines for implementing the Privacy Act of 1974. [Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1975. 20 p. (Federal information processing standards publication. FIPS pub. 41).

U.S. Office of Federal Register. Protecting Your Right to Privacy. Washington, U.S. Govt. Print. Off., 1976.

U.S. Office of Management and Budget. Privacy Act implementation; guidelines and responsibilities. Federal register, v. 40, July 9, 1975: 28947-28978.

III. Computers and Privacy

Canada. Department of Communications and Department of Justice. Privacy and Computers. Ottawa, Information Canada, 1972. 236 p.

Computer data bank privacy controversy revisited: an analysis and an administrative proposal. Catholic University law review. v. 22, Spring, 1973: 628.

Hamilton, Peter. Computer security. Philadelphia, Auerbach Publ., 1973. 122 p.

IBM Corporation. Data Security and Data Processing: Study of Specific Aspects of Data Security. White Plains, N.Y., IBM Corporation, 1974. 1253 p.

Martin, James. Security, accuracy, and privacy in computer systems. Englewood Cliffs, N.J., Prentice-Hall Inc., [1973] 626 p.

Nolan, Richard L. Personal privacy versus the corporate computer. Harvard business review, v. 53, Mar.-Apr. 1975: 62-70.

Turn, Rein. Privacy and Security in Personal Information Data bank Systems. Santa Monica, the Rand Corporation, 1974. 104 p.

U.S. Congress. House. Committee on Government Operations. Federal information systems and plans, implications and issues. Hearings, 93d Congress, 2d session. Part 3. Washington, U.S. Govt. Print. Off., 1974. 1214 p.
Hearings held Jan. 29, 31, and Feb. 5, 1974.

_____. _____. _____. Subcommittee on Foreign Operations and Government Information. Records maintained by government agencies. Washington, U.S. Govt. Print. Off., 1972. 92d Congress, 2d session. 232 p.

U.S. Congress. Senate. Committee on Government Operations.
Privacy and protection of personal information in Europe: privacy developments and their implications for United States policy: a staff report. Washington, U.S. Govt. Print. Off., 1975. 436 p.
At head of title: 93d Cong., 2d sess. Committee print.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Federal data banks and constitutional rights; a study of data systems on individuals maintained by agencies of the United States Government. 93d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1974. 6 v. (3527 p.)

_____. _____. _____. Subcommittee on Constitutional Rights.
Federal data banks and constitutional rights: a study of data systems on individuals maintained by agencies of the United States Government. Washington, U.S. Govt. Print. Off., 1974. 53 p.
At head of title: 93d Cong., 2d sess. Committee print.

_____. _____. _____. Subcommittee on Constitutional Rights.
Federal data banks, computers and the Bill of Rights. Hearings, 92d Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1971. 1047-2164 p.
Hearings held Feb. 23...Mar. 17, 1971.
Part II--relating to Departments of Army, Defense, and Justice.

U.S. Department of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems.
Records computers and the rights of citizens. Washington, U.S. Govt. Print. Off., 1973. 346 p.

Ware, Willis H. Data Banks, Privacy, and Society. Report No. 5131. Santa Monica, the Rand Corporation, 1973. 11 p.

Westin, Alan F. and Michael A. Baker. Project directors. Data banks in a free society. Computers, record-keeping and privacy. Report of the Project on Computer Data banks of the Computer Science and Engineering Board National Academy of Science. New York, N.Y. Quadrangle Books, 1972. 522 p.

Westin, Alan F. Information technology in a democracy. Cambridge. Harvard University Press, 1971. 499 pages.

Wheeler, Stanton, ed. On Record: files and dossiers in American life. New York, Russell Sage Foundation, 1969.

Younger, K., Chairman. Report of the Committee on Privacy. London, Her Majesty's Stationery Office, 1972. 350 pages.

IV. Credit Reports and Electronic Funds Transfer

Dunkelberg, William C. Credit use and users: the value of credit use. Journal of consumer credit management, v. 4, winter 1973: 66-80.

Ege, Stephen M. Electronic funds transfer: a survey of problems and prospects in 1975. Maryland law review, v. 35, no. 1, 1975: 3-56.

Foer, Albert A. The Personal Information Market: An Examination of the Scope and Impact of the Fair Credit Reporting Act. Loyola Law Students Consumer Journal, v. II, 1974: 37-138.

Hendrickson, Robert. The Cashless Society. New York, Dodd, Mead & Co, 1972.

Knight, Robert E. The changing payments mechanism: electronic funds transfer arrangements. Federal Reserve Bank of Kansas City monthly review, July-Aug. 1974: 10-20.

Little (Arthur D.) Inc. The consequences of electronic funds transfer; a technology assessment of movement toward a less cash/less check society. Washington, National Science Foundation, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1975. 351 p.
"NSF/RA/X-75-015"

McLaughlin, Marsha Morrow. Vaupel, Suzanne. Constitutional right of privacy and investigative consumer reports: little brother is watching you. Hastings constitutional law quarterly, v. 2, summer 1975: 773-828.

U.S. Congress. House. Committee on Banking, Currency and Housing. Subcommittee on Consumer Affairs.
The Fair Credit Billing Act amendments of 1975. Hearing, 94th Cong., 1st sess., on H.R. 10209. Oct. 23, 1975. Washington, U.S. Govt. Print. Off., 1975. 115 p.

63-619 O - 76 - 82

U.S. Congress. Senate. Committee on Banking, Housing and Urban Affairs. Subcommittee on Consumer Credit. Credit Reporting Abuses. Hearings, 93d Congress, 2d session, on amending the Fair Credit Reporting Act. February 5, 1974. Washington: U.S. Government Printing Office, 1974. 54 p.

_____. _____. _____. Subcommittee on consumer Credit. Fair Credit Reporting Act of 1973. Hearings, 93d Congress, 1st session, on S. 2360. [Washington, U.S. Govt. Off., 1973] 993 p.

_____. _____. _____. Subcommittee on Consumer Affairs.
Fair Credit reporting amendments of 1975. Hearings, 94th Cong., 1st sess., on S. 1840. Washington, U.S. Govt. Print. Off., 1976. 987 p. Hearings held Oct. 22...Nov. 18, 1975.

_____. _____. _____.
Subcommittee on Financial Institutions. Electronic Funds Transfer Moratorium Act of 1975. Hearing, 94th Cong., 1st sess., on S. 245. Mar. 14, 1975. Washington, U.S. Govt. Print. Off., 1975. 221 p.

Westermeier, John T., Jr. The Privacy Side of the Credit Card, American University Law Review, v. 23, Fall 1973: 183-207.

V. Criminal Justice Records

"Arrest Records--Protecting the Innocent Misuse of Arrest Records." Tulane Law Review 48 April, 1974: 629.

"Branded: Arrest Records of the Unconvicted." Mississippi Law Journal v. 44 November, 1973: 928.

Cohn, Sigmund A. "Criminal Records--a Comparative Approach." Georgia Journal of International and Comparative Law, v. 4 Winter, 1974: 116.

"Criminal Law--Expungement of Arrest Records." New York Law Forum, Summer, 1975: 85.

DeWeese, J. Taylor. "Reforming Our 'Record Prisons': a Proposal for the Federal Regulation of Crime Data Banks." Rutgers Camden Law Journal, v. 21 Summer, 1974: 26.

Hill, J. Graham. Texas Open Records Act: law enforcement agencies' investigatory records. Southwestern law journal, v. 29, spring 1975: 431-453.

Project SEARCH. Committee on Security and Privacy. Security and Privacy Considerations in Criminal History Information Systems. Technical Report No. 2, July, 1970. [Sacramento, California., California Crime Technological Research Foundation, 1970]. 55 p.

"Protection of Privacy of Computerized Records in the National Crime Information Center," University of Michigan Journal of Law Reform, v. 7, Spring, 1974: 594.

Rehnquist, William H. "Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or, Privacy, You've Come a Long Way, Baby." Kansas Law Review, v. 23, Fall, 1974: 1.

SEARCH Group, Inc. Standards for Security and Privacy of Criminal Justice Information. Technical Report No. 13. [Sacramento, Calif., 1975]. 30 p.

U.S. Congress. House. Security and Privacy of Criminal Arrest Records. Hearings before Subcommittee No. 4 of the Committee on the Judiciary, House of Representatives, on H.R. 13315, 92nd Cong., 2d sess., 1972.

_____. _____. Committee on Internal Security. Domestic Intelligence Operations for Internal Security Purposes, Part I. Hearings, 93d Congress, 2d session. Feb. 20, April 1, 2, 8, and June 4 and 5, 1974. Washington, U.S. Govt. Print. Off., 1974. 3913 p.

_____. _____. Committee on the Judiciary. Subcommittee on Civil Rights and Constitutional Rights. Dissemination of Criminal Justice Information. Hearings, 93d Congress, 2d sess. on H.R. 188, H.R. 9783, H.R. 12574, and H.R. 12575. July 26, Aug. 2, Sept. 26, Oct. 11, 1973; Feb. 26, 28, Mar. 5, 28, and April 3, 1974. Washington, U.S. Govt. Print. Off., 1974. 586 p.

_____. _____. _____. Subcommittee on Civil and Constitutional Rights.
FBI oversight. Hearings, 94th Cong., 1st sess. Part I. Feb. 27, 1975. Washington, U.S. Govt. Print. Off., 1975. 48 p. "Serial no. 2"

U.S. Congress. Senate. Criminal Justice Data Banks--1974. Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, Senate, on S. 2542, S. 2810, S. 2963, and S. 2964, 93rd Cong., 2d sess., 1974. 2 vols.

_____. _____. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Criminal Justice Information and Protection of Privacy Act of 1975. Hearings, 94th Cong., 1st sess., on S. 2008, S. 1427, and S. 1428. July 15-16, 1975. Washington, U.S. Govt. Print. Off., 1975. 311 p.

U.S. Dept. of Justice. Criminal justice information systems. Federal register, v. 40, May 20, 1975: 22113-22119.

U.S. General Accounting Office. How Criminal Justice Agencies Use Criminal History Information; Report to the Senate Subcommittee on Constitutional Rights, Committee on the Judiciary, by the Comptroller General of the United States. [Washington, 1974]. (B-171019 Aug. 19, 1974).

U.S. Law Enforcement Assistance Administration. Office of General Counsel. Compendium of state laws governing the privacy and security of criminal justice information. Washington, 1975. 1 v.

Walz, Kathleen. "Arrest Record Expungement in California: the Polishing of Sterling." 9 University of San Francisco Law Review 299 (Fall, 1974).

VI. Financial Privacy

Association of the Bar of the City of New York. Committee on Civil Rights. The privacy of Federal income tax returns: committee report. Record of the Association of the Bar of the City of New York, v. 30, May-June 1975: 400-408.

Callaghan, Thomas A., Jr. The Comptroller of the Currency's disclosure regulation and a banker's right to privacy. Banking law journal, v. 92, Feb. 1975: 119-139.

Fighting conflicts of interest in officialdom: constitutional and practical guidelines for state financial disclosure laws. Michigan law review, v. 73, Mar. 1975: 758-781.

Government Access to Bank Records. Note. Yale Law Journal, v. 83, 1974: 1439-1474.

U.S. Congress. House. Committee on Banking, Currency and Housing. Subcommittee on Financial Institutions Supervision, Regulation and Insurance. Bank failures, regulatory reform, financial privacy. Hearings, 94th Cong., 1st sess., on H.R. 8024. 3v. June 26, July 14, 15, 16, 17, and 21, 1975. Washington, U.S. Govt. Print. Off., 1975. 2234 p.

_____. _____. Committee on Ways and Means. Subcommittee on Oversight. Proposals for administrative changes in Internal Revenue Service procedures. Hearings, 94th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1975. 434 p. Hearings held July 10...Sept. 22, 1975.

U.S. Congress. Joint Committee on Internal Revenue Taxation. Confidentiality of tax returns. Washington, U.S. Govt. Print. Off., 1975. 44 p. At head of title: Committee print.

_____. Investigation of the Special Service Staff of the Internal Revenue Service. Prepared for the Joint Committee on Internal Revenue Taxation. Washington, U.S. Govt. Print. Off., 1975. 114 p.
At head of title: 94th Cong., 1st sess. Committee print.

U.S. Congress. Senate. Committee on Finance. Subcommittee on Administration of the Internal Revenue Code.
Federal tax return privacy. Hearings, 94th Cong., 1st sess. Washington, U.S. Govt. Print. Off., 1975. 308 p.
Hearings held Apr. 21 and 28, 1975.

_____. _____. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure.
IRS disclosure. Hearings, 93d Cong., 2d sess. Washington, U.S. Govt. Print. Off., 1974. 294 p.
Hearings held Apr. 1 and July 31, 1974.

_____. _____. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Political intelligence in the Internal Revenue Service: the Special Service Staff; a documentary analysis. Washington, U.S. Govt. Print. Off., 1974. 344 p.

VII. Public Officials

Gay, M. Lee, Jr. Privacy of information in Florida public employee personnel files. University of Florida law review, v. 27, winter 1975: 481-501.

Little, Joseph W. Tompkins, Thomas. Open government laws: an insider's view. North Carolina law review, v. 53, Feb. 1975: 451-489.

U.S. Congress. House. Committee on Government Operations. The use of polygraphs and similar devices by Federal agencies; thirteenth report together with separate and dissenting views. Washington, U.S. Govt. Print. Off., 1976. 61 p. (94th Cong., 2d sess. House. Report no. 94-795)

_____. _____. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
The use of polygraphs and similar devices by Federal agencies. Hearings, 93d Cong., 2d sess. June 4 and 5, 1974. Washington, U.S. Govt. Print. Off., 1974. 790 p.

_____. _____. Committee on Post Office and Civil Service. Subcommittee on Retirement and Employee Benefits.
Rights to privacy of Federal employees. Hearings, 93d Cong., 1st and 2d sess., on H.R. 1281 and related bills. Washington, U.S. Govt. Print. Off., 1974. 378 p.
Hearings held May 14, 1973...Aug. 8, 1974.
"Serial no. 93-22"

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights.
Privacy, polygraphs, and employment; a study. Washington, U.S. Govt. Print. Off., 1974. 18 p.
At head of title: 93d Cong., 2d sess. Committee print.

VIII. Government Surveillance

Association of the Bar of the City of New York. Committee on Federal Legislation.
Judicial procedures for national security electronic surveillance. Record of the Association of the Bar of the City of New York, v. 29, Dec. 1974: 751-774.

Christie, George C. Government Surveillance and Individual Freedom: A Proposed Statutory Response to Laird v. Tatum and the Broader Problem of Government Surveillance of the Individual. New York University Law Review, v. 47, Nov. 1972: 871-902.

Donner, Frank. Electronic surveillance: the national security game. Civil liberties review, v. 2, no. 3, 1975: 15-47.

Ehlke, Richard. Political Surveillance and Police Intelligence Gathering--Rights, Wrongs, and Remedies. Wisconsin Law Review, 1972: 175-199.

Ervin, Sam J., Jr. Privacy and government investigations. University of Illinois law forum, v. 1971, 1971: 137-153.

U.S. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights. Telephone monitoring practices by Federal agencies. Hearings, 93d Congress, 2d session. June 11 and 13, 1974. Washington, U.S. Govt. Print. Off., 1974. 293 p.

_____. _____. Committee on the Judiciary.
Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance; report to accompany H.R. 15173. Washington, U.S. Govt. Print. Off., 1974. 5 p.
93d Cong., 2d sess. House. Report no. 93-1343.

_____. _____. Committee on the Judiciary. Subcommittee on Courts, Civil Liberties, and the Administration of Justice.
Wiretapping and electronic surveillance. Hearings, 93d Cong., 2d sess., on H.R. 1597, H.R. 7773, H.R. 9781, H.R. 9815, H.R. 9973, H.R. 10008, H.R. 10331, H.R. 11629, H.R. 11836, and H.R. 13825. Apr. 24, 26, and 29, 1974. Washington, U.S. Govt. Print. Off., 1974. 275 p.
"Serial no. 41"

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Criminal justice data banks--1974. Hearings, 93d Congress, 2d session, on S. 2542, S. 2810, S. 2963, S. 2964. Mar. 5, 6, 7, 12, 13, [and] 14. Washington, U.S. Govt. Print. Off., 1971. 733 p.

_____. Federal data banks, computers, and the Bill of Rights. Hearings, 92d Congress, 1st session on S. 969, S. 975, S. 1550, S. 2546. Washington, U.S. Govt. Print. Off., 1971. 2164 p.
Hearings held Feb. 23-25, Mar. 2, 3, 4, 9, 11, 15 [and] 17, 1971.

_____. Military surveillance. Hearings, 93d Congress, 2d session, on S. 2318. Apr. 9, 10, 1974. Washington, U.S. Govt. Print. Off., 1974. 397 p.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures.
Electronic surveillance for national security purposes. Hearings, 93d Cong., 2d sess., on S. 2820, S. 3440, and S. 4062. Oct. 1, 2, and 3, 1974. Washington, U.S. Govt. Print. Off., 1975. 577 p.

IX. Emerging Areas of Record Privacy

Beytagh, Francis X. Privacy and a free press: a contemporary conflict in values. New York law forum, v. 20, Winter 1975: 453-514.

Hirsch, Phil. The World's Biggest Data Bank. Datamation, v. 16, May 1970: 66-73.

Kaiser, Barbara L. Patients' Rights of Access to their Own Medical Records: The Need for New Law, Winter 1975: 317-330.

Kauffman, Miles P. Welfare and the right to privacy; applicants' rights. Res ipsa loquitur, v. 25, fall 1972: 107-113.

McNamara, Robert M., Jr. and Joyce R. Starr. Confidentiality of Narcotic Addict Treatment Records. Columbia Law Review, v. 73, Dec. 1973: 1579-1612.

Mattessich, Carole Marie. The Buckley Amendment: Opening School Files for Student and Parental Review, Catholic University Law Review, v. 24, Spring 1975: 588-603.

Mironi, Mordechai. The Confidentiality of Personnel Records: A Legal and Ethical View, Labor Law Journal, v. 25, May, 1974: 270-292.

Steinberg, Joseph. Some Aspects of Statistical Data Linkage for Individuals. In Data Bases, Computers, and the Social Sciences. New York, John Wiley and Sons, Intersciences Division, 1970. p. 238-251.

Stern, Laurence C. Medical Information Bureau: The Life Insurer's Data bank, v. 4, Rutgers Journal of Computers and the Law, v. 4, 1974: 1-41.

U.S. Congress. House. Committee on Government Operations. Foreign Operations and Government Information Subcommittee.
Sale or distribution of mailing lists by Federal agencies. Hearings, 92d Cong., 2d sess., on H.R. 8903 and related bills. Jan. 13 and 15, 1972. 362 p.

_____. _____. Committee on Post Office and Civil Service. Census confidentiality/mid-decade sample survey bill; report to accompany H.R. 14153. Washington, U.S. Govt. Print. Off., 1971. 27 p. 92d Congress, 2d session. House. Report no. 92-1288).

U.S. Congress. Joint Economic Committee. Subcommittee on Economic Statistics. The coordination and integration of government statistical programs. Hearings, 90th Congress, 1st session. Washington, U.S. Govt. Print. Off., 1967. 206 p.
Hearings held May 17, 18; June 7, 8, 1967.

U.S. Dept. of Health, Education, and Welfare. Office of the Secretary.
Privacy rights of parents and students. Federal register, v. 40, Jan. 6, 1975: 1207-1216.

U.S. Office of Science and Technology. Privacy and Behavioral Research. Washington, U.S. Govt. Print. Off., 1967.

U.S. President's Commission on Federal Statistics. Federal Statistics. 2 vols. Washington, D. C.: U.S. Government Printing Office, 1971.

Jerome Hanus
Analyst, American National Government
Government Division
March 2, 1976

APPENDICES

Appendix A

Citizen Access to Records: A Guide to Federal Statutory Requirements

(By Jerome Hanus, Analyst in American National Government, Government Division, Congressional Research Service)

The rapid proliferation, at the Federal level, of data banks in the 1960's and 1970's—containing in excess of 1¼ billion separate records on American residents—lent substance to the worries of many that the nation's tradition of limited government was in jeopardy. In response, the propriety of overextensive governmental and corporate information gathering and disclosure is being reconsidered. Congress has reflected this concern by enacting the Freedom of Information Act (FOIA), as amended (5 U.S.C. 552), which requires disclosure, with certain exemptions, of records and information held by the Federal Government. In addition, Congress passed three laws which authorize access to certain personally identifiable records held by credit corporations and by the Federal Government. These are: The Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), the Family Educational Rights and Privacy Act of 1971 (20 U.S.C. 1232g) which is referred to below as the Buckley Amendment, and the Privacy Act of 1974 (5 U.S.C. 552a).

Together these laws lay the foundation for a code of fair information practices by which citizens and others can exercise a measure of control over the collection of information about themselves. The principles evolving from the legislation are those requiring records to be kept with accuracy, relevancy, and fairness. But these principles can become effective only if citizens are aware of their rights and act on behalf of them. This report is designed to assist congressional personnel in advising constituents about their rights over information held by Government and by private credit corporations. Key provisions of each of the Acts are described below.

I. TYPES OF RECORDS COVERED

Fair Credit—applies to any information bearing on a consumer's eligibility for credit, insurance, employment, rent, license, or government benefit. However, medical records are not included in disclosure provisions. [15 U.S.C. 1681g]

Buckley Amendment—applies to most personal records maintained by educational institutions receiving Federal funding. [20 U.S.C. 1232g (a)]

FOIA—with certain exceptions, applies to all governmental records which do not fall within one of the exemptions listed in the Act. [5 U.S.C. 552]

Privacy Act—with certain exceptions, applies to all Federal records held by Federal executive authorities, including personnel records, which are retrievable by a personal identifier such as a name or number. [5 U.S.C. 552a (a)]

II. BENEFICIARIES OF THE ACTS

Fair Credit—an individual consumer on whom a consumer report has been made. [15 U.S.C. 1681a (b)]

Buckley Amendment—parents or legal guardians of a student under 18 years of age, or a student 18 years or older. [20 U.S.C. 1232g (e)]

FOIA—any individual or institution. [5 U.S.C. 552]

Privacy Act—a citizen of the U.S. or an alien lawfully admitted for permanent residence. [5 U.S.C. 552 (a)]

III. INSTITUTIONS COVERED

Fair Credit—consumer reporting agencies and persons (including corporations) who procure or cause to be prepared an investigative consumer report on any consumer for use by a third party. [15 U.S.C. 1681d]

Buckley Amendment—educational agencies or institutions which are the recipients of Federal educational funds. [20 U.S.C. 1232g (a)(3)]

FOIA—all Federal agencies and departments including the U.S. Postal Service, the Postal Rate Commission, and Government corporations as well as contractors who operate an information system on behalf of a Federal agency. [5 U.S.C. 552 (e)]

Privacy Act—all Federal Executive agencies and departments including the U.S. Postal Service, the Postal Rate Commission, and Government corporations as well as contractors who operate an information system on behalf of a Federal agency. The CIA, FBI, and other law enforcement agencies are permissively exempt from the disclosure requirement. [5 U.S.C. 552a (a)]

IV. NOTIFICATION TO THE INDIVIDUAL

Fair Credit—a person who procures, or causes to be prepared, an investigative consumer report on a consumer, must disclose to the consumer that such a report is being made. The consumer must be notified in writing no later than three days after the date on which the report was requested; the consumer must also be notified of his right to request additional information. [15 U.S.C. 1861d]

Buckley Amendment—specifies that students and their parents must be informed of their rights under this Act. The notification must include:

(*a*) the types of education records, and information contained in them, maintained by the institution;

(*b*) the name and position of the official who has custody of the information, the names of persons who have access, and the purposes for which they have access;

(*c*) the policies of the institution for reviewing and expunging those records;

(*d*) the procedures for obtaining access to records;

(*e*) the process for challenging the content of the records;

(*f*) the cost for reproducing records;

(*g*) the categories which the institution has defined as "directory information" (i.e., information which the institution will disclose publicly);

(*h*) notice under this Act must be in the language of the student or parent;

(*i*) notice must be given at least annually.

FOIA—the Act is not intended to furnish notification to specific individuals. A person seeking information from a Federal agency should consult the *Federal Register* and agency indexes which provide information for the public as to any matter issued, adopted, or promulgated after July 4, 1967. [5 U.S.C. 552 (a)]

Privacy Act—each agency that maintains a system of records is required to inform each individual whom it asks to supply information, on the form which it uses to collect this information or on a separate form that can be retained by the individual, of the authority which authorizes the request for the information and whether disclosure is mandatory or voluntary; the principal purpose or purposes for which the information is intended to be used; the routine uses which may be made of the information; and the effects on him, if any, of not providing all or any part of the requested information. [5 U.S.C. 552a (e)(3)] Agencies must also publish in the *Federal Register* at least annually a notice of the existence and character of the system of records and any routine uses to which they are put. [5 U.S.C. 552a (e)(4), (11)]

V. TO WHOM REQUEST IS DIRECTED

Fair Credit—to the appropriate consumer reporting agency, such as a credit bureau. [15 U.S.C. 1681d (b)]

Buckley Amendment—to the appropriate educational institution or agency. [20 U.S.C. 1232g (a)(1)(A)]

FOIA—to the officer or office specified in the appropriate agency's procedures published in the *Federal Register* or to the agency itself. [5 U.S.C. 552 (a)]

Privacy Act—to the officer or office specified in the appropriate agency's procedures published in the *Federal Register* or to the agency itself. [5 U.S.C. 552a (d)(f)]

VI. TIME PERIOD FOR RESPONSE TO REQUESTS TO EXAMINE RECORDS

Fair Credit—notice that a consumer report is being prepared must be mailed to the consumer no more than three days after the date on which the report was first requested. A consumer's request for disclosure must be responded to within five days after the request was made. [15 U.S.C. 1681 (a) (b)]

Buckley Amendment—an educational agency or institution must respond to a request for access to records within forty-five days after the request has been made. With respect to "directory information," the agency or institution must allow a "reasonable" period of time, after giving public notice of the categories of information to be disclosed, for a parent or guardian to inform the institution or agency that any or all of the information designated should not be released without the parent's consent. [20 U.S.C. 1232g (a) (5) (B)]

FOIA—the Act specifies: Each agency, upon any request for records must determine within ten work-days whether to comply with the request and must immediately notify the person making the request of the determination. The agency must make a determination with respect to any appeal within twenty working days. Under usual circumstances, the agency may have a ten day extension by giving written notice to the requester. [5 U.S.C. 552(a) (6)]

Privacy Act—the Act does not prescribe a specific time for response, but Federal regulations suggest a response to the inquiry within ten working days. Upon request by an individual for amendment of a record pertaining to him, the agency must acknowledge in writing receipt of the request within ten work-days. If the request is denied, the requestor may ask for review of the denial. A final determination of the request must be made within thirty work-days with a possible thirty-day extension for "good cause." [5 U.S.C. 552a (d)]

VII. COST OF DOCUMENTS

Fair Credit—no charge to the consumer for the report if he requests disclosure within thirty days after receipt of a notification from the reporting agency or notification from a debt collection agency affiliated with the agency stating that his credit rating may be or has been adversely affected. Otherwise, the agency may impose a reasonable charge for the disclosure. [15 U.S.C. 1681j]

Buckley Amendment—specific provisions concerning charges are not included.

FOIA—each agency is ordered to specify a uniform schedule of fees. The fees are to be limited to reasonable standard charges for document search and duplication and to provide for recovery of only the direct costs of such search and duplication. Documents are to be furnished without charge or at a reduced charge where the agency determines that waiver or reduction of the fee is in the public interest. [5 U.S.C. 552(a) (4) (A)]

Privacy Act—an agency may charge fees for making copies of an individual's record, excluding the cost of any search for, and review of, the record. [5 U.S.C. 552a (f)]

VIII. JUDICIAL REVIEW

Fair Credit—a consumer may bring action in any appropriate district court of the United States to enforce liability under the Act. Actual damages may be obtained as well as reasonable attorney fees as determined by the court. [15 U.S.C. 1681p]

Buckley Amendment—no specific provisions for resort to the courts. However, access would be available after exhaustion of administrative remedies. [20 U.S.C. 1232g (g)]

FOIA—a complainant may request an appropriate district court of the United States to enjoin an agency from withholding records and to order their production. In such a case, the court shall determine the matter *de novo*,[1] *and* may examine the contents of such agency records *in camera*[2] to determine whether the agency properly withheld such records under any of the exemptions listed in the Act. The burden is on the agency to justify its action.

[1] This means the court will take a new and independent look at the facts.
[2] *In camera* mean the judge will review the records in his private chambers and not in open court.

The agency is required to answer the complaint within thirty days of service of the complaint unless the court directs otherwise. Proceedings and appeals take precedence on the docket over all cases and must be assigned for hearing and trial or for argument at the earliest practicable date. The court may assess against the United States reasonable attorney fees and other litigation costs. If the court finds for the complainant and issues a written finding that the circumstances surrounding the withholding raise questions as to whether agency personnel acted arbitrarily or capriciously, the Civil Service Commission must promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer who was primarily responsible for the withholding. The Commission must submit its findings and recommendations to the administrative authority of the agency concerned which shall then take the corrective action that the Commission recommends. In the event of noncompliance with the order of the court, the district court may punish the responsible employee for contempt. [5 U.S.C. 552 (a)]

Privacy Act—an individual may bring a civil action against the agency in an appropriate district court. In a suit in which the agency has refused to *amend* the individual's record in accordance with his request, the court may order the agency to do so and the court shall determine the matter *de novo*. The court may assess against the United States reasonable attorney fees and other litigation costs when the complainant has substantially prevailed. In a suit to enjoin the agency from *withholding* records, the court shall determine the mater *de novo* and may examine the contents of the agency records *in camera* to determine whether the records may be withheld under any of the exemptions of the Act. If the court determines that the agency acted willfully, the United States shall be liable for actual damages to the individual with a minimum recovery of $1000; and the costs of the action together with reasonable attorney fees. An agency officer or employee who knowingly or willfully maintains or discloses records prohibited under this Act shall be guilty of a misdemeanor and fined not more than $5000. [5 U.S.C. 552a (g) (h) (i)]

APPENDIX B

[From the Michigan Law Review, May–June 1975]

II. Increasing Protection of Citizen Privacy

A. *Introduction*

The subcommittee, under your able direction, has been conducting hearings for over a year now on failures by the Federal Government to make information available to the public. You are to be commended for your efforts because, surely, there is no single attribute more fundamental to a democratic society than the free flow of information. Liberty and freedom are dependent upon the truth.

There is another side of this issue, however, which deserves

> equal respect and examination—the right of individuals to maintain personal privacy. . . . [I]nvasion of the sanctity of a person's privacy will be as destructive of a society's freedom and liberty as will the foreclosure of information about the acts of government in such a society.[1499]

When President Johnson signed the Federal Public Records Act into law, he expressed pride in "an open society in which the people's right to know is cherished and guarded."[1500] The federal and state governments have figured prominently in the controversy over the "right to know," as government operations have become increasingly numerous, complex, and removed from public scrutiny. Governmental growth, with its attendant increase in information needs, has also given rise to crusaders for the necessary complement of the right to know—the right of privacy.

The long-standing tension between governmental information needs and the desire of individuals to withhold personal, identifying details about their lives has heightened in the past several decades as a result of the interplay of three developments. First, these years have witnessed a geometric growth in government regulation and services that have increased government-citizen contacts. Second, acceptance of the behavioral-predictive theory of information—the theory that behavior patterns can be predicted if enough relevant data is gathered and properly analyzed[1501]—has led to demands for increasing amounts of information in ever widening areas.[1502] Third, rapid advances in computer science have eliminated the traditional hindrances to government acquisition of data[1503] by increasing the ease of information acquisition, lessening the need to limit data retention,[1504] and increasing intragovernmental transfer of informa-

1499. *Sale or Distribution of Mailing Lists by Federal Agencies, Hearings on H.R. 8903 and Related Bills Before a Subcomm. of the House Comm. on Government Operations*, 92d Cong., 2d Sess. 77 (1972) (statement of Representative Goldwater) [hereinafter *Hearings on Mailing Lists*].

1500. ATTORNEY GENERAL'S MEMORANDUM, *supra* note 309, at II (statement of President Johnson).

1501. *See* A. WESTIN, PRIVACY AND FREEDOM 135-57 (1967).

1502. *See* Ervin, *Privacy and Government Investigations*, 1971 U. ILL. L.F. 137, 138. *See also* NATIONAL ACADEMY OF SCIENCES, DATABANKS IN A FREE SOCIETY xvii (A. Westin & M. Baker eds. 1972) [hereinafter DATABANKS]; House Republican Research Committee, Task Force on Privacy, Recommendations, Aug. 21, 1974, at 1.

1503. For a full discussion of the impact of computers see A. MILLER, ASSAULT ON PRIVACY 1-53, 322 (1971).

1504. *See Federal Data Banks, Computers and the Bill of Rights, Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. 943 (1971) [hereinafter *Hearings on Data Banks*] (statement of C. Lister); DATABANKS, *supra* note 1502, at 320 ("The National Academy of Sciences reported in 1972 that it is now technologically possible to build a computerized on-line file containing the compacted equivalent of 20 pages of typed information about the personal history and selected activities of every person in the United States").

Data that might once have been discarded are now more likely to be kept, in an

tion.[1505] As Professor Miller has pointed out: "In accordance with a principle akin to Parkinson's Law, as capacity for information-handling increases there is a tendency to engage in more extensive manipulation and analysis of data . . . pertaining to a larger number of variables."[1506] Together, these three phenomena have created a spiraling demand for information and have left us threatened with the emergence of a "dossier society."

1. *The Extent of Government-Held Information*

Government data acquisition statistics make clear that not only political activists and government employees are threatened by the accumulation of information by the government. Increasingly, access to government benefits and services requires a willingness on the part of individuals to divulge private information.[1507] Moreover, an observable trait of government agencies is that when a problem is confronted, the tendency is to react with a demand for more data,[1508] as evidenced by the 1970 census[1509] and the rising number of government questionnaires.[1510]

In 1966, in the midst of debate over the proposed National Data Center, a Senate Judiciary subcommittee initiated a survey to determine "the amount, nature, and use of information which Government agencies currently maintain on individuals."[1511] The survey revealed that federal files contained more than 3 billion records on individual citizens,[1512] nearly one half of which were retrievable by computer, including over 27.2 billion names, 2.3 billion present and past addresses, 264 million criminal histories, 280 million mental

---

expectation that a purpose may ultimately be found for them. In fact, it has been suggested that the ability of a computer to store large quantities of data compels the owner to increase data acquisition in order to reduce the cost per unit of data. *See* Report of Secretary's Advisory Committee on Automated Personal Data Systems, HEW, Records, Computers and the Rights of Citizens 13 (1973) [hereinafter HEW Report]. Computerization also permits more complete use of the information gathered, and facilitates the tasks of retrieving and disseminating: Data may be more imaginatively collated and collections may be searched for relatively low priority purposes. *Hearings on Data Banks, supra*, at 943.

1505. *See* A. WESTIN, *supra* note 1501, at 161-62; A. MILLER, *supra* note 1503, at 24-54. *But see* DATABANKS, *supra* note 1502, at 253, 255.

1506. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society*, 67 MICH. L. REV. 1089, 1103 (1969).

1507. Miller, *supra* note 1506, at 1103.

1508. *Hearings on Data Banks, supra* note 1504, at 942-43 (statement of C. Lister).

1509. *See Privacy, the Census and Federal Questionnaires, Hearings on S. 1791 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 91st Cong., 2d Sess. 460-95 (1969) [hereinafter *Hearings on the Census*].

1510. *See, e.g., Hearings on the Census, supra* note 1509, at 37-53, 867-926.

1511. STAFF OF SUBCOMM. ON ADMINISTRATIVE PRACTICE AND PROCEDURE OF THE SENATE COMM. ON THE JUDICIARY, 90TH CONG., 2D SESS., GOVERNMENT DOSSIER 1 (Comm. Print 1967) [hereinafter GOVERNMENT DOSSIER].

1512. *See id.* at 9.

health records, 916 million profiles on alcoholism and drug addiction, and over 1.2 billion financial records.[1513] More significantly, the report concluded that much of the information retained was irrelevant to agency needs and that in many instances confidentiality provisions were nonexistent or not meaningful.[1514] A 1974 survey by a different subcommittee, which supplemented and updated these findings, pointed out that 86 per cent of the government data banks are computerized, and that few of the data banks had any explicit statutory authorization for their retention of files.[1515] Computerization, however, cannot itself account for the abundance of government-held data concerning individual citizens: According to at least one study, for most organizations computerization has not brought an increase in scope of the content of records maintained on each individual.[1516]

It has been estimated that the average American is the subject of ten to twenty personal files or dossiers compiled by either government units or private organizations.[1517] The threat to individual privacy is thus no longer a potential—it is a reality.[1518] As Senator Mathias aptly described the situation, "If knowledge is power, this encyclopedic knowledge gives Government the raw materials of tyranny."[1519]

2. *A Definition of Privacy*

The counterweight to this growing governmental power is the developing concern over privacy. A definition of privacy that will provide a conceptually sound basis for the development of rules con-

1513. *Hearings on Data Banks, supra* note 1504, at 574.

1514. GOVERNMENT DOSSIER, *supra* note 1511, at 8. Further, as Representative Horton pointed out: "Even if . . . the most sensitive and personal information is shielded in confidence . . . large additional reservoirs of data on individual citizens are not only not secure but actually available for public disclosure for purposes of commercial or other types of solicitation." *Hearings on Mailing Lists, supra* note 1499, at 63.

1515. *See* STAFF OF SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS: SUMMARY AND CONCLUSIONS 10-11, 26-29 33-35 (Comm. Print 1974) [hereinafter SUMMARY AND CONCLUSIONS]. Besides tabulating the amount of information held by agencies, the study of this committee, in six volumes, analyzes the information-gathering practices of all government agencies with respect to statutory authority, subject notification, subject review, access by other agencies, public access, security precautions, and sources of information. *See* STAFF OF SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS (Comm. Print 1974) [hereinafter FEDERAL DATA BANKS].

1516. *See* DATABANKS, *supra* note 1502, at 244.

1517. *See Records Maintained by Government Agencies, Hearings on H.R. 9527 and Related Bills Before a Subcomm. of the House Comm. on Government Operations*, 92d Cong., 2d Sess. 22 (1972) (statement of Representative Patten) [hereinafter *Hearings on Records*].

1518. *Hearings on Mailing Lists, supra* note 1499, at 63 (statement of Representative Horton).

1519. *Hearings on Data Banks, supra* note 1504, at 574.

cerning information practices is difficult to formulate because the significance of privacy protection varies for each individual and with each individual circumstance.[1520] Further, privacy collides with other social values that have proved equally difficult to define, such as freedom of the press and freedom of information.[1521] Nevertheless, to determine the degree to which government must respect privacy, it is necessary to establish a working definition.[1522]

Since Warren and Brandeis seized upon Judge Cooley's definition of privacy as the "right to be let alone,"[1523] numerous persons have attempted to sophisticate a privacy doctrine.[1524] Clearly, privacy interests of the individual are many and varied. At issue in this discussion are privacy interests relating to government information-handling and the individual's desire to maintain anonymity with regard to personal, identifying details. A useful definition, therefore, is one in which a number of writers have concurred: the right of privacy is the right to control the flow of information concerning the details of one's individuality—one's physical and individual characteristics, knowledge, capabilities, beliefs, and opinions.[1525] In specifying the areas protected by the privacy right, however, legislatures and courts have invariably turned to a right of privacy based on the content of the information: only certain categories of information—information regarding the family or individual sexuality, for example—are protected.[1526] But the underlying privacy concept, which is tied to the individual and his personality, has a considerably

---

1520. HEW Report, *supra* note 1504, at 38.

1521. *Id.*

1522. Pipe, *Privacy: Establishing Restrictions on Government Inquiry*, 18 AM. U. L. REV. 516, 518 (1969).

1523. *See* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, at 193 (1890).

1524. *See, e.g.*, A. MILLER, *supra* note 1503, at 210-38; A. WESTIN, *supra* note 1501, at 31-51, 330-99; Fried, *Privacy*, 77 YALE L.J. 175, 182 (1968); Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275 (1974).

1525. *See* A. MILLER, *supra* note 1503, at 25 ("[P]rivacy is the individual's right to control the circulation of information relating to him . . ."); Fried, *supra* note 1524, at 483 ("Privacy, thus, is control over knowledge about oneself"); Comment, *Maintenance and Dissemination of Criminal Records: A Legislative Proposal*, 19 UCLA L. REV. 654, at 654 n.2 (1972) ("The right of privacy is the right of the individual to decide for himself how much he will share with others his thoughts, his feelings, and the facts of his personal life"). *Cf.* Justice Douglas' definition of privacy as having a "dual aspect: [E]very individual needs both to communicate with others and to keep his thoughts and beliefs from others. This means that a person should have the freedom to select for himself the time and circumstances when he will share his thoughts and attitudes with others and to determine the extent to which that sharing will go." Douglas, *Foreword* to Project, *The Computerization of Government Files: What Impact on the Individual?*, 15 UCLA L. REV. 1374, 1375 (1968). A broad view of privacy would also require that a person who discloses information to another be able to control the latter's disposition of that information.

1526. *See* 5 U.S.C. § 552(b)(6) (1970), discussed in the text at notes 700-44 *supra*; text at notes 1562-788 & 1897-902 *infra*.

broader reach and thus has a significant potential for development and expansion, as the Privacy Act of 1974 illustrates.[1527]

3. *Government Invasions of Privacy: Methods and Results*

There are three major stages in any information-handling system: acquisition, retention, and dissemination. Government information practices may threaten the individual's control over the flow of information about himself at any of these stages; thus, four questions are raised: What information may be collected; under what circumstances may it be retained; to whom may the data be made available; and what remedies or sanctions are available to secure effective protection for privacy.

The question of acquisition is the most crucial because all other problems come into play only after information is obtained. Government agencies "tend to defend needs for information with a pledge of confidentiality of personal reports once secured, omitting the fact that intrusions on a person's privacy begin at the taking of sensitive personal facts."[1528] Problems of acquisition have provoked considerable discussion. For example, certain questions asked of applicants for federal jobs have been challenged,[1529] and several questions were removed from the proposed 1970 census after an outcry from persons protesting the sensitivity of the questions.[1530] Even if the collection of certain information would not violate individual privacy rights, the methods employed to collect it, such as wiretapping and electronic surveillance,[1531] may constitute such a violation.

Retention and dissemination of acquired information pose equally grave threats. The retention of certain criminal justice[1532] and welfare data[1533] has become a prominent concern; in fact, the controversy that first focused attention on the right of privacy—the National Data Bank proposal—involved the place of retention.[1534] A problem that arises in the area of dissemination is that one agency that may legitimately collect and retain certain information on an individual, may, without the individual's consent, give the informa-

---

1527. *See* text at notes 1966-2214 *infra*.

1528. *Hearings on the Census*, *supra* note 1509, at 130 (Representative Betts). *See id.* at 270-82 (testimony of L. Speiser, ACLU).

1529. *See* text at notes 2031-43 *infra*.

1530. *See* text at notes 1990-93 *infra*.

1531. *See* text at notes 1844-48 *infra*; *Hearings on Military Surveillance Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974) [hereinafter *Hearings on Military Surveillance*].

1532. *See, e.g.*, Tarleton v. Saxbe, 507 F.2d 1116 (D.C. Cir. 1974).

1533. *See* text at notes 1709-18 *infra*.

1534. *See* FEDERAL DATA BANKS, *supra* note 1515; notes 2102-04 *infra* and accompanying text.

tion to an agency that could not have legitimately collected it. The 1974 Senate survey of agency practices found this danger quite real: "Once information about an individual is collected by a Federal agency, it is likely that that information will be fairly readily passed on to other Federal, State and local agencies."[1535] Finally, privacy interests are often further infringed when an individual whose privacy has been invaded is denied a remedy.

The harms from unregulated government information-handling can be divided into three categories: psychological problems created by acquisition of data, loss of individual benefits due to misuse of the data, and invasion of privacy per se. Any attempt to appraise the impact on individuals of data acquisition must consider the potential psychological harms. First, there is the very real possibility that individuals will, with increasing frequency, base their decisions regarding activities and expressions on how they will enhance their record.[1536] A concern for a clean record, reinforced by the popular conception of the computer as unforgetting,[1537] could threaten to create "a society in which unorthodoxy is discouraged by its notoriety, and even the mildest eccentricities are catalogued for official evaluation."[1538] This "chilling effect" on unpopular expressions and beliefs exemplifies the theory of "aversive control" avoidance-learning—that as an individual learns to avoid activities that he feels are disapproved, he will stop not only the disapproved activities, but similar or related activities as well.[1539] In the extreme, individuals may begin to doubt whether they exist apart from their record.[1540]

A 1952 study evaluating the impact of governmental loyalty and security inquiries found many resulting behavioral changes: severance of membership in organizations on the Attorney General's list and cancellation of subscriptions to literature sent by these organizations; refusal to sign petitions without proof of a bona fide sponsorship; refusal to join an organization not on the Attorney General's list for fear it might later develop in a radical direction; and cautiousness in political conversations with strangers.[1541] Moreover, it

---

1535. SUMMARY AND CONCLUSIONS, *supra* note 1515, at 37.

1536. A. MILLER, *supra* note 1503, at 50.

1537. This has been described as an "information prison" in which a person's past places inescapable limits on his future. *See Hearings on Data Banks, supra* note 1504, at 943 (testimony of C. Lister, ACLU).

1538. *Id.*

1539. *See* A. BANDURA, PRINCIPLES OF BEHAVIOR MODIFICATION 293-354 (1969).

1540. A. MILLER, *supra* note 1503, at 49.

1541. *See* Johoda & Cook, *Security Measures and Freedom of Thought: An Exploratory Study of the Impact of Loyalty and Security Programs*, 61 YALE L.J. 295, 307-08 (1952). For a detailed treatment of the chilling effect of surveillance on legitimate political activity see Askin, *Surveillance: The Social Science Perspective*, in

has been observed that surveillance of a particular individual need not actually be going on to produce the effect in that individual as long as there is public knowledge that surveillance has occurred and is continuing to occur.[1542] This is especially relevant because of recent surveys revealing widespread public concern over the threat to privacy from computers.[1543] Privacy is necessary for proper psychological development,[1544] for health,[1545] and for the growth of democratic societies.[1546] Yet, as Richard L. Tobin commented in a 1968 editorial entitled "1984 Minus Sixteen and Counting," "[w]e cannot assume . . . that privacy will survive simply because man has a psychological or social need for it."[1547]

Even certain decisions of federally elected officials seem "chilled" by various surveillance and information-keeping techniques. The *New York Times* stated on February 25, 1974:

> The source recalled one Senator who had been told of an investigation concerning his daughter, a college student who had "gotten involved in demonstrations and free love," and a Republican Representative who had been told that the [FBI] possessed evidence indicating that he was a homosexual.
>
> "We had him in our pocket after that," the source said of the Representative. He added that he could not recall the Senator, a liberal Democrat, ever criticizing the FBI in public.[1548]

But, as Representative Mikva, himself the subject of an Army intelligence file pointed out:

> The objection to this program is not that a U.S. Senator may have

---

SURVEILLANCE, DATAVEILLANCE AND PERSONAL FREEDOMS 72-86 (COLUM. HUMAN RIGHTS L. REV. ed. 1973).

1542. *See* Askin, *supra* note 1541, at 82.

1543. For example, a national survey conducted in 1971 found that 53 per cent of the sample believed that computerized information files might be used to destroy individual freedoms, and 58 per cent felt that computers will be used in the future to keep people under surveillance. In addition 38 per cent believed that computers represent a real threat to personal privacy, 91 per cent of those questioned felt that computers were used to compile information files on U.S. citizens, and 54 per cent believed these files were maintained for surveillance of activist or radical groups. Finally, 62 per cent expressed their concern over the types of information being kept, and 45 per cent said political activity records should not be kept. *Id.* at 88.

1544. *Cf.* Handler & Hollingsworth, *Stigma, Privacy, and Other Attitudes of Welfare Recipients*, 22 STAN. L. REV. 1, 2 (1969).

1545. Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROB. 307, 318 (1966).

1546. A. WESTIN, *supra* note 1501, at 34.

1547. Tobin, *1984 Minus Sixteen and Counting*, SATURDAY REV., April 13, 1968, at 77-78.

1548. Crewdson, *Files from Hoover to Backers Reported*, N.Y. Times, Feb. 25, 1974, at 52, col. 1 (late city ed.), *quoted in* 120 CONG. REC. H2440 (daily ed. April 2, 1974). *See Hearings on Data Banks*, *supra* note 1504, at 137 (statement of Representative Mikva).

been subjected to surveillance, or that a special file was or was not kept on him . . . .

The harm comes rather when the ordinary citizen feels he cannot engage in political activity without becoming a "person of interest," without having his name and photo placed in a file colloquially, if not officially, labeled "subversive."[1549]

Invasions of privacy also result in direct injury to the individual through misuse of his records, for once an individual divulges personal information, he in most instances loses all effective control over it.[1550] Harm can result if information that is accurate from one perspective is used in a different context in which it is misleading. Harm can also result from incomplete or erroneous information collections. These possibilities are aggravated because in many situations individuals have only limited rights to see, supplement, or correct their records.[1551]

Damages flowing from the use of incomplete information are clear: In 1973, Massachusetts Governor Sargent gave a full pardon to a former felon who had kept his record clean for 10 years. The individual moved to a community 1000 miles away and enrolled in a community college. The college president, after running a routine police check with the state's new computer file, learned of his conviction and expelled him. The computer record had not included the full pardon.[1552] Another case was related by Representative Moss:

A young couple were returning home to San Francisco one evening a year ago when they were stopped by Santa Clara County Sheriff's deputies, eventually handcuffed, held at gunpoint and locked up overnight on charges of auto theft. The arresting officers had queried the San Francisco city and county criminal justice data bank and learned that the couple's Falcon had been reported stolen a year earlier. Police had failed to enter into the computer the "pink slip" record that the car had been recovered by its rightful owners.[1553]

There are countless similar examples of individuals being denied employment, promotion, or some other benefit because of records of prior arrests.[1554] That charges were dropped or dismissed, or that

1549. *Hearings on Data Banks, supra* note 1504, at 89.

1550. *Criminal Justice Data Banks, Hearings on S. 2542, S. 2810, S. 2963, S. 2964 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary.* 93d Cong., 2d Sess. 18 (1974) (statement of Senator Ervin) [hereinafter *Hearings on Criminal Justice Data Banks*].

1551. *See, e.g.*, text at notes 1678-93 *infra*. The new federal Privacy Act takes steps to provide rights of access and challenge for records held by the federal government. *See* text at notes 2084-98 *infra*.

1552. 120 CONG. REC. H2459 (daily ed. April 2, 1974) (remarks of Representative Heinz).

1553. *Id.* at H2456.

1554. *See Hearings on Criminal Justice Data Banks, supra* note 1550, at 5-7 (statement of Senator Ervin).

the person was found not guilty, is often not added to the record.[1555] The injuries resulting from inaccurate information are similar. An employer in Texas managed to get the arrest record of one Tosh from a friend on the Fort Worth police department. He displayed mug shots and rap sheets to discourage voting for the union Tosh was organizing. The record being displayed was for one Charles Tosch, however, a convicted felon. Tosh, the organizer, had been arrested on minor charges and released.[1556]

The following sections of this Project discuss the development of a right of privacy in state and federal law. Using as an analytical framework the four questions regarding the threats posed by government information-practices to individual privacy, the discussion examines consecutively the common-law privacy tort,[1557] state statutes,[1558] the federal constitutional law,[1559] federal statutes prior to the enactment of the Privacy Act of 1974,[1560] and, finally, the new Privacy Act,[1561] to see how the balance has been struck between the governmental need for information and individual privacy, and to see the extent to which these areas of the law provide adequate protection from the above-mentioned harms. Although the focus of the discussion is on federal law, state statutes and the common law are included in order to give a more complete picture of the themes underlying the development of legal protections for privacy.

1555. *See id.* at 19.

1556. 120 Cong. Rec. H2452 (daily ed. April 2, 1974) (statement of Representative Moss).

1557. *See* text at notes 1564-625 *infra.*

1558. *See* text at notes 1626-788 *infra.*

1559. *See* text at notes 1789-915 *infra.*

1560. *See* text at notes 1916-65 *infra.*

1561. *See* text at notes 1966-2214 *infra.*

C. *The Federal Constitutional Law of Privacy*

1. *Inherent Limitations on the Federal Government's Power To Collect Information*

The federal government is restricted to operating within the powers enumerated in the Constitution—a restriction that constitutes an inherent limitation on information collection by both Congress and the executive branch. While the power of Congress to collect information[1789] is nowhere specifically enumerated, it has

1789. *See generally* M. DIMOCK, CONGRESSIONAL INVESTIGATING COMMITTEES (1929); E. EBERLING, CONGRESSIONAL INVESTIGATIONS (1928); M. MCGEARY, THE DEVELOPMENTS OF CONGRESSIONAL INVESTIGATIVE POWER (1940); Alfange, *Congressional Investigations and the Fickle Court*, 30 U. CIN. L. REV. 113 (1961); Boudin, *Congressional and Agency Investigations: Their Uses and Abuses*, 35 VA. L. REV. 143 (1949); Coudert, *Congressional Inquisition and Individual Liberty*, 15 VA. L. REV. 537 (1929); Cousens, *The Purpose and Scope of Investigations Under Legislative Authority*, 26 GEO. L.J. 905 (1938); Driver, *Constitutional Limitations on the Power of Congress To Punish Contempts of Its Investigating Committees*, 38 VA. L. REV. 887 (1952); Ford, *The Lawyer and the Congressional Investigation*, 21 S. CAL. L. REV. 242 (1948); Gose, *The Limits of Congressional Investigating Power*, 10 WASH. L. REV. 61 (1935); Hamilton, *The Inquisitorial Power of Congress*, 23 A.B.A.J. 511 (1937); Landis, *Constitutional Limitations on the Congressional Power of Investigation*, 40 HARV. L. REV. 153 (1926); Lashley, *The Investigating Power of Congress: Its Scope and Limitations*, 40 A.B.A.J. 763 (1954); Loring, *Powers of Congressional Investigation Committees*, 8 MINN. L. REV. 595 (1924); Massey, *Congressional Investigations and Individual Liberties*, 25 U. CIN. L. REV. 323 (1956); Merry, *The Investigating Power of Congress: Its Scope and Limitations*, 40 A.B.A.J. 1073 (1954); McGeary, *The Congressional Power of Investigation*, 28 NEB. L. REV. 516 (1949); Moreland, *Congressional Investigations and Private Persons*, 40 S. CAL. L. REV. 189 (1967); Tunstall, *The Investigating Power of Congress: Its Scope and Limitations*, 40 VA. L. REV. 875 (1954).

been found to exist by implication as a necessary adjunct to the exercise of those powers that are enumerated.[1790] There are five express powers from which congressional authority to collect information can be implied: the powers to enumerate the population,[1791] to impeach,[1792] to judge congressional election returns,[1793] to discipline and expel members of Congress,[1794] and to legislate.[1795] The census clause of the Constitution literally permits merely an enumeration of "free Persons . . . excluding Indians not taxed,"[1796] although the census has in fact been used extensively as a means of collecting information from the citizenry.[1797] The Supreme Court has not yet ruled whether the census power will support collection of information unrelated to actual enumeration,[1798] and the deliberations of the framers are unrevealing.[1799] One could logically conclude that the scope of the census power is limited to an actual counting. The Second Circuit, however, has held that the express language of the

---

1790. The seminal case concerning implied powers is McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316 (1819). For a discussion of implied powers in the context of the collection of information see McGrain v. Daugherty, 273 U.S. 135, 160-75 (1927).

1791. U.S. CONST. art. I, § 2, cl. 3, requires: "The actual Enumeration shall be made within three years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct."

1792. U.S. CONST. art. I, § 2, cl. 5, provides: "The House of Representatives . . . shall have the sole Power of Impeachment." U.S. CONST. art. I, § 3, cl. 6, provides: "The Senate shall have the sole Power to try all Impeachments."

1793. U.S. CONST. art. I, § 5, cl. 1, provides: "Each House shall be the Judge of the Elections, Returns and Qualifications of its own Members . . . ."

1794. U.S. CONST. art I, § 5, cl. 2, provides: "Each House may . . . punish its Members for disorderly Behaviour, and, with the Concurrence of two thirds, expel a Member."

1795. U.S. CONST. art. I, § 1, provides: "All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives." Legislative powers are enumerated more specifically in U.S. CONST. art. I, § 8.

1796. U.S. CONST. art. I, § 2, cl. 3.

1797. *See Hearings on the Census*, *supra* note 1509, at 460 (memorandum from the Census Bureau). *See also* Fernandez, *The Census*, 42 S. CAL. L. REV. 245 (1969); text at notes 1925-38 *infra*; notes 1990-93 *infra* and accompanying text.

1798. The Court, in Knox v. Lee, 79 U.S. (12 Wall.) 457, 536 (1870) (Legal Tender Cases) noted in dictum:

> [A] power may exist as an aid to the execution of an express power, or an aggregate of such powers, though there is another express power given relating in part to the same subject but less extensive. Another illustration of this may be found in connection with the provisions respecting a census. The Constitution orders an enumeration of free persons in the different States every ten years. The direction extends no further. Yet Congress has repeatedly directed an enumeration not only of free persons in the States but of free persons in the Territories, and not only an enumeration of persons but the collection of statistics respecting age, sex, and production. Who questions the power to do this?"

1799. *See* 1 THE RECORDS OF THE FEDERAL CONVENTION OF 1787, 600-06 (M. Farrand ed., rev. ed. 1937). The debates do not indicate the intended scope of the census power. The primary discussions related to problems of representation, *i.e.*, whether wealth was a proper measure and who would be counted.

Constitution limiting the census to an enumeration "does not prohibit the gathering of other statistics, if 'necessary and proper,' for the intelligent exercise of other powers enumerated in the constitution, and in such case there could be no objection to acquiring this information through the same machinery by which the population is enumerated . . . ."[1800]

An implied power to investigate exists under each of the other four powers. It is available to Congress for the purpose of collecting information necessary to an informed exercise of those powers,[1801] but is limited by the breadth of the express functions to which it attaches. Three of these express functions—the power to impeach, the power to judge congresional election returns, and the power to discipline and expel members of Congress—are judicial in nature.[1802] Because Congress is primarily a legislative body and because the three judicial powers reserved to Congress are extremely limited in scope, the investigative powers arising under these functions will be used in far fewer instances than the investigative power falling under the legislative function.[1803]

The parameters of the investigative power inferred from the legislative function were established in *Kilbourn v. Thompson*[1804] and *McGrain v. Daugherty*.[1805] Prior to 1880, the courts had given Congress almost unlimited power to investigate,[1806] but in *Kilbourn*, the Supreme Court upheld a citizen's right not to respond to congressional subpoenas issued in an investigation in furtherance of an illegitimate purpose. The Court noted that the inquiry could not be "simply a fruitless investigation into the personal affairs of indi-

---

1800. United States v. Moriarity, 106 F. 886, 891 (2d Cir. 1901).

1801. Concerning investigations relating to the power to legislate see Eastland v. United States Servicemen's Fund, Inc., 43 U.S.L.W. 4635, 4639-40 (U.S. May 27, 1975); McGrain v. Daugherty, 273 U.S. 135 (1927); text at notes 1804-19 *infra*. Concerning investigations relating to the power to judge congressional election returns see Barry v. United States *ex rel.* Cunningham, 279 U.S. 597 (1929). Concerning investigations relating to the power to discipline and expel members of Congress see *In re* Chapman, 166 U.S. 661, 668 (1897). *See generally* Moreland, *supra* note 1789.

1802. Barry v. United States *ex rel.* Cunningham, 279 U.S. 597, 613 (1929).

1803. Although it is clear that the power of investigation exists under the impeachment clause, no cases have arisen on this matter. *See* Moreland, *supra* note 1789, at 224. Barry v. United States *ex rel.* Cunningham, 279 U.S. 597 (1929), is the only case directly concerning the investigative power pursuant to the congressional authority to judge election returns, although both United States v. Norris, 300 U.S. 564 (1937), and Roudebush v. Hartke, 405 U.S. 15 (1972), indicated that such a power exists. Finally, other than Powell v. McCormack, 395 U.S. 486 (1969), which assumes but does not discuss the investigative power, *In re* Chapman, 166 U.S. 661 (1897), is the sole Supreme Court case on investigations relating to the authority to discipline and expel members. United States v. Brewster, 408 U.S. 501 (1972), does, however, discuss in dictum the nature and extent of the congressional power to discipline members.

1804. 103 U.S. 168 (1880).

1805. 273 U.S. 135 (1927).

1806. *See* Moreland, *supra* note 1789, at 189-211, and cases cited therein.

viduals,"[1807] but must be capable of resulting in "valid legislation on the subject to which the inquiry referred."[1808] In *McGrain*, the Court upheld subpoenas issued in an investigation of the Justice Department for the purpose of formulating reform legislation. The Court reasoned that "[a] legislative body cannot legislate wisely or effectively in the absence of information respecting the conditions which the legislation is intended to affect or change."[1809] It is today clear that the legislative power "encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes . . . , includes surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them . . . , [and] comprehends probes into departments of the Federal Government to expose corruption, inefficiency or waste."[1810] Thus, while the requirement of a proper legislative purpose constitutes a restraint on Congress, the sphere of legitimate legislative activity, as the Court suggested recently in *Eastland v. United States Serivcemen's Fund*,[1811] is sufficiently broad to justify an inquiry into almost any question of national interest.

A further limitation on the congressional investigative power is that all questions must be pertinent to the asserted legislative purpose.[1812] When an investigation is conducted by either the full House or Senate this limitation is of little consequence since Congress'

1807. 103 U.S. at 195.

1808. 103 U.S. at 195. Of interest are the conflicting interpretations given *Kilbourn* by the majority and concurring opinions in Eastland v. United States Servicemen's Fund, 43 U.S.L.W. 4635 (U.S. May 27, 1975), discussed in the text at notes 1873-76 *infra*. In *Kilbourn* the House of Representatives attempted to punish an individual for contempt for refusal to comply with a congressional subpoena. The Court invalidated the House's effort, reasoning that the subject matter of the investigation was judicial and not legislative, and that the House had thus "assumed a power which could only be properly exercised by another branch of the government . . . ." 103 U.S. at 192. The majority in *Eastland* stated that the subpoena at issue in *Kilbourn* was subject to attack because it was not essential to legislating. 43 U.S.L.W. at 4640. The concurring opinion of Justices Marshall, Brennan, and Stewart, however, stated that the individual in *Kilbourn* was able to attack the subpoena because his suit was brought against the House Sargeant at Arms, who was carrying out the unconstitutional directive, rather than against House members or their legislative aides. 43 U.S.L.W. at 4643. The concurring justices thus sought to emphasize that congressional subpoenas within the legislative sphere are subject to attack as long as Congressmen or their aides are not the parties defendant.

1809. 273 U.S. at 175. The Court also observed: "In actual legislative practice power to secure needed information . . . has long been treated as an attribute of the power to legislate. It was so regarded in the British Parliament and in the Colonial legislatures before the American Revolution; and a like view has prevailed and been carried into effect in both houses of Congress and in most of the state legislatures." 273 U.S. at 161.

1810. Watkins v. United States, 354 U.S. 178, 187 (1957).

1811. 43 U.S.L.W. 4635, 4639-41 (U.S. May 27, 1975).

1812. *See* Sinclair v. United States, 279 U.S. 263 (1929). *See also* Deutch v. United States, 354 U.S. 178 (1957). The pertinency requirement has been codified at 2 U.S.C. § 192 (1970).

power to legislate in so many areas virtually ensures that there will be a proper legislative purpose to which almost any question could be pertinent.[1813] Most investigations, however, are carried out by congressional committees[1814] or federal agencies[1815] to which Congress has delegated its investigatory power for specific purposes through authorizing resolutions or statutes.[1816] Authorizing resolutions are often broad in scope, but there is at least a minimal requirement that such resolutions delineate the agency's "jurisdiction and purpose with sufficient particularity" to ensure that compulsory process is used only in furtherance of a legislative purpose,[1817] and at times agency investigations exceeding the bounds of congressional authorizations have been disallowed and witnesses permitted to forgo responding to inquiries.[1818] While Congress can amend delegating legislation to enable questions to satisfy the purpose and pertinancy requirements, amending resolutions or legislation require considerable congressional effort and are unlikely to be enacted except in cases of great concern. Where a witness objects to the pertinancy of a question at a committee hearing, "unless the subject matter has been made to appear with undisputable clarity, it is the duty of the investigative body . . . to state for the record the subject under inquiry at that time and the manner in which the propounded questions are pertinent thereto."[1819] On the basis of this requirement, which is derived from the due process clause of the fifth amendment, the Court on several occasions has reversed contempt convictions resulting from refusals to answer investigative in-

---

1813. *See* Barry v. United States *ex rel.* Cunningham, 279 U.S. 597 (1929).

1814. *See, e.g.*, Barenblatt v. United States, 360 U.S. 109 (1959); Watkins v. United States, 354 U.S. 178 (1957).

1815. *See, e.g.*, United States v. Morton Salt Co., 338 U.S. 632 (1950); Electric Bond & Share Co. v. SEC, 303 U.S. 419 (1938); Sinclair v. United States, 279 U.S. 263 (1928); ICC v. Brimson, 154 U.S. 447 (1894). *See also* Note, *Investigatory Powers of Congress and Administrative Agencies*, 26 WASH. U. L.Q. 531 (1941). Congress' power of investigation was held to be delegable to federal administrative agencies in ICC v. Brimson, 154 U.S. 447 (1894).

1816. For codified examples of congressional delegation of investigatory powers to administrative agencies see 26 U.S.C. § 7602 (1970) (examination of books, papers, or records to ascertain the accuracy of any tax return); 44 U.S.C. §§ 3501-11 (1970) (procedure to be followed by federal agencies in collecting information, including hearings as to the necessity of such collection). *See generally* 13 U.S.C. §§ 41, 44, 61, 62, 101, 102, 131, 141, 142, 161, 301 (1970) (permitting Census Bureau to collect information unrelated to enumeration).

1817. Watkins v. United States, 354 U.S. 178, 201 (1957). *See* Barenblatt v. United States, 360 U.S. 109 (1959); United States v. Rumely, 345 U.S. 41 (1953).

1818. Several early cases disallowed agency investigations exceeding the bounds of congressional authorities. *See, e.g.*, Harriman v. ICC, 211 U.S. 407 (1908); United States v. Louisville & N. R.R., 236 U.S. 318 (1915); FTC v. American Tobacco Co., 264 U.S. 298 (1924). *See* Mechem, *Fishing Expeditions by Commissions*, 22 MICH. L. REV. 765 (1924).

1819. Watkins v. United States, 354 U.S. 178, 214-15 (1957).

quiries:[1820] because a witness can object to questions on pertinancy grounds, fundamental fairness requires that he not be placed in jeopardy of a contempt citation without being afforded the opportunity to judge for himself the question's pertinancy.

The executive branch's power to investigate is similarly expansive, derived principally from the President's authority to "take Care that the Laws be faithfully executed."[1821] The scope of the President's investigatory power under this provision, while not yet tested in the courts,[1822] is presumably limited only by the same purpose and pertinancy requirements that limit congressional investigations.[1823] Because of the myriad laws to enforce, however, these requirements are only minor restrictions. This power to investigate is apparently subject to narrowing by Congress since Congress can revoke any law it enacts and can presumably, therefore, revoke executive power to collect information necessary to enforce any law.[1824]

2. *The Constitutional Right of Disclosural Privacy*

In interpreting certain provisions of the Bill of Rights to protect the individual from governmental intrusions, the Supreme Court has spoken broadly of a right of privacy. Although there is no explicit constitutional recognition of such a right, the Court "has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."[1825] A right of privacy has been found in the fourth amendment,[1826] the first amendment,[1827] penumbras emanating from the first eight amend-

---

1820. *See, e.g.*, Watkins v. United States, 354 U.S. 178 (1957). *See also* Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963); Sweezy v. New Hampshire, 354 U.S. 234 (1957). *But see* Uphaus v. Wyman, 360 U.S. 72 (1959).

1821. U.S. CONST. art. II, § 3. The power to investigate may also be implied from other constitutionally enumerated powers of the President, such as the power of pardon granted in U.S. CONST. art. II, § 2.

1822. In Laird v. Tatum, 408 U.S. 1 (1972), the plaintiffs challenged an Army civilian-surveillance program used to gather information allegedly necessary to an intelligent use of force in cases of civil disorder. The Court, holding the case nonjusticiable because the record showed no objective harm, noted that "it is significant that the principle sources of information were the news media and publications in general circulation." 408 U.S. at 6. This statement implies that the executive's use of the investigative power does not clearly controvert plaintiff's rights so long as the information was already public. The concept of "public facts" is rooted in the common law of privacy. *See* text at notes 1584-90 *supra*.

1823. *See* text at notes 1804-20 *supra*.

1824. The limitations on the *manner* in which the executive can collect information imposed by statutes such as the Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. §§ 2511, 2516-18 (1970), evidence the truth of this proposition.

1825. Roe v. Wade, 410 U.S. 113, 152 (1973).

1826. *See* Katz v. United States, 389 U.S. 347 (1967).

1827. *See* Stanley v. Georgia, 394 U.S. 557 (1969); NAACP v. Alabama, 357 U.S. 449 (1958); Watkins v. United States, 354 U.S. 178 (1957).

ments,[1828] the ninth amendment,[1829] and the concept of ordered liberty guaranteed by the due process clauses of the fifth and fourteenth amendments.[1830] Significantly, in discussing the right of privacy, the Court has not distinguished between disclosural privacy—the right to control the flow of information concerning the details of one's individuality[1831]—and that aspect of privacy concerning the individual's ability to decide whether to perform certain acts or to undergo certain experiences, an aspect accurately characterized as privacy relating to personal autonomy.[1832] Many of these cases, especially the "privacy cases,"[1833] have focused on the privacy of autonomy. It is the purpose of this section to analyze the degree of protection for disclosural privacy offered by each of the constitutional sources of privacy protection,[1834] to determine whether these separate protections are capable of being generalized into a unitary right of disclosural privacy, and to ascertain when government interests in information acquisition, retention, and dissemination will override individual privacy interests.

Except for the third amendment's ban on the quartering of soldiers in any house without the owner's consent in times of peace—a very narrow prohibition—the fourth amendment comes closer to mentioning a right of privacy than any other provision of the Con-

---

1828. *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

1829. *See* Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (Goldberg, J., concurring).

1830. *See* Roe v. Wade, 410 U.S. 113 (1973). *See also,* Beaney, *The Constitutional Right to Privacy in the Supreme Court,* 1962 SUP. CT. REV. 212.

1831. *See* text at note 1525 *supra*. Note that the term "privacy" as defined here is not necessarily the same as the right that is protected at common law. *See* text at notes 1562-625 *supra*.

1832. *Compare* Katz v. United States, 389 U.S. 347 (1967) (disclosure), *with* Roe v. Wade, 410 U.S. 113 (1973) (autonomy). For a discussion of the disclosure-autonomy distinction see Beardsley, *Privacy: Autonomy and Selective Disclosure,* in PRIVACY 56 (J. Pennock & J. Chapman eds. 1971). *See also* Greenawalt, *The Right of Privacy,* in THE RIGHTS OF AMERICANS 299 (N. Dorsen ed. 1971); Gross, *The Concept of Privacy,* 42 N.Y.U. L. REV. 34 (1967); Note, *supra* note 1720; Note, *Roe and Paris: Does Privacy Have a Principle?,* 26 STAN. L. REV. 1161 (1974).

1833. *See, e.g.,* Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965). *See* text at notes 1877-902 *infra*.

1834. The fifth amendment privilege against self-incrimination does deal with an individual's interest in disclosural privacy, *cf.* Boyd v. United States, 116 U.S. 616 (1886); Mapp v. Ohio, 367 U.S. 643, 661-65 (1961) (Black, J., concurring), but the privacy protection afforded by that amendment is minimal because incriminating testimony can be compelled if either use or transactional immunity from prosecution is conferred on the witness. *See* Kastigar v. United States, 406 U.S. 441 (1972); Zicarelli v. State Commn. of Investigation, 406 U.S. 472 (1972). The fifth amendment privilege against self-incrimination also does not apply to the compelled production of privately held but legally required records. Wilson v. United States, 221 U.S. 361, 380 (1911). Nor does the privilege apply "to records required by law to be kept in order that there may be suitable information of transactions which are the appropriate subjects of governmental regulation . . . ." Wilson v. United States, 221 U.S. 361, 380 (1911). *See also* Davis v. United States, 328 U.S. 582 (1946).

stitution.[1835] An examination of some of the principal search and seizure cases suggests a broad concern for privacy underlying the fourth amendment. For example, in *Boyd v. United States*[1836] the Court struck down a statute empowering a court to require a defendant to produce personal papers; it reasoned that the essence of an unreasonable search and seizure is "not the breaking of his doors, and the rummaging of his drawers, . . . but . . . the invasion of his indefeasible right of personal security, personal liberty and private property . . . ."[1837] In holding that the fourth amendment limits the compulsory production of evidence in addition to prohibiting unlawful searches,[1838] the Court provided protection for a privacy concept broad enough to include both disclosure and autonomy.[1839]

In *Olmstead v. United States*,[1840] the Supreme Court retreated from the broad formulation of *Boyd* to a mechanistic interpretation of the fourth amendment by sanctioning a home telephone tap that did not constitute a technical trespass. Chief Justice Taft, writing for the Court, interpreted the fourth amendment as forbidding only "an actual physical invasion of [one's] house."[1841] By emphasizing the manner rather than the effect of the invasion, the holding narrowed the concept of privacy underlying the fourth amendment. In

---

1835. The fourth amendment to the Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *See generally* A. AMSTERDAM, FEDERAL CONSTITUTIONAL RESTRAINTS ON SEARCH, SEIZURE, ARREST, DETENTION AND INTERROGATION BY STATE LAW ENFORCEMENT OFFICERS (1966); P. GAY, THE POLICEMAN AND THE ACCUSED (1965); L. KOLBREK & G. PORTER, THE LAW OF ARREST, SEARCH, AND SEIZURE (1965); N. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION (1937); Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974); Note, *The Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J. L. REF. 154 (1972).

1836. 116 U.S. 616 (1886).

1837. 116 U.S. at 630.

1838. *See, e.g.*, Gouled v. United States, 255 U.S. 298 (1921); *Ex parte* Jackson, 96 U.S. 727 (1878). *But cf.* Carroll v. United States, 267 U.S. 132 (1925).

1839. *Boyd* demonstrates that the fourth amendment serves two purposes: the protection of individual privacy and the protection of the individual against the compulsory production of evidence to be used against him, as well as against unlawful searches. *See* Davis v. United States, 328 U.S. 582, 587 (1946). Based on this dual purpose analysis, one could argue that the "right to be let alone" attaches only in a criminal context, since, as the Court noted in *Boyd*, the fourth and fifth amendments "run almost into each other." 116 U.S. at 630. However, the inference that privacy is fully protected by the fourth amendment only when the individual is suspected of criminal activity was rejected by the Court in Camara v. Municipal Court, 387 U.S. 523 (1967).

1840. 277 U.S. 438 (1928). *Cf.* Silverman v. United States, 365 U.S. 505 (1961) (slight physical penetration of premises by a spike microphone constitutes a technical trespass and, if made without a warrant, is an illegal search).

1841. 277 U.S. at 466.

an often-quoted dissent, Justice Brandeis adhered to the broader view:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfaction of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[1842]

One author interpreted Justice Brandeis' construction of the fourth amendment to require that "all government intrusions on a person's privacy at home, in his papers and effects, and on his free movement would have . . . to be justified, with the government forced to bear the burden of showing why a particular form of interference was reasonable. Privacy, though not absolute, would have a high place in the hierarchy of protected values."[1843]

In *Katz v. United States*,[1844] the Court returned to a more expansive view of the fourth amendment by excluding evidence obtained by the use of an electronic listening and recording device attached to the outside of a public phone booth. Abandoning the *Olmstead* trespass doctrine,[1845] the Court based its decision on the sweeping proposition that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[1846] The fourth amendment applied in this instance, the Court stated, because the defendants had "justifiably relied"[1847] upon the privacy afforded by the public phone booth. In his concurrence, Justice Harlan understood the Court's holding to require

> first that a person have exhibited an actual (subjective) expectation

1842. 277 U.S. at 478.

1843. Beaney, *supra* note 1830, at 227.

1844. 389 U.S. 347 (1967).

1845. 389 U.S. at 353. The Court refused to overrule *Olmstead* expressly, but Justice Harlan, concurring, felt that *Olmstead*, "which essentially rested on the ground that conversations were not subject to the protection of the Fourth Amendment" had been overruled. 389 U.S. at 362 n.*.

1846. 389 U.S. at 351-52.

1847. 389 U.S. at 353.

63-629 O - 76 - 34

> of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[1848]

While the *Katz* view of the privacy concept underlying the fourth amendment goes only to disclosure and not to autonomy, and is therefore not as broad as the implications of *Boyd*, the decision suggests that the fourth amendment—equally applicable in the noncriminal context[1849]—gives rise to a zone of privacy adhering to the individual,[1850] at times even in situations outside the home.[1851] Because the test turns on what society deems a reasonable expectation of privacy, the individual of course receives more protection within his home than without, in accordance with the common law prior to the Constitution.[1852] But, while applicable in a broad range of contexts, this fourth amendment right of disclosural privacy affords minimal protection because it must yield in the face of reasonable government intrusion. While the fourth amendment has been interpreted to require probable cause or a warrant for searches in the criminal context[1853] and in administrative searches involving physical intrusions by government agents into the home,[1854] it is satisfied in the case of questionnaires if the information sought is "reasonably

---

1848. 389 U.S. at 361.

1849. *See* Camara v. Municipal Court, 387 U.S. 523 (1967); Frank v. Maryland, 359 U.S. 360, 377 (1959) (Douglas, J., dissenting).

1850. The notion of a "zone of privacy" outside the home was apparently rejected in Paris Adult Theatre I v. Slaton, 413 U.S. 49, 66 (1973). However, unlike *Katz*, which was a disclosure case, *Paris* involved the privacy of autonomy. Petitioners in *Paris* had been enjoined by the Georgia supreme court from exhibiting two allegedly obscene films. They argued that the constitutional doctrine of privacy laid down in Stanley v. Georgia, 394 U.S. 557 (1969), where the Court held that the possession of obscene materials in the home was beyond the reach of the state's criminal law because the Constitution protected the right to receive information and ideas and to be generally free from government intrusion, applied outside the home as well. The Court rejected this extension of *Stanley*, holding that the privacy of the home could not be equated with a general zone of privacy that follows a consumer of obscene materials wherever he goes. 413 U.S. at 66. These cases indicate that certain aspects of privacy of autonomy, while protected inside the home, are not necessarily protected outside the home. The privacy of disclosure, however, is oriented to the person, not to the place, and thus should follow the individual wherever he may be. Thus, *Paris* should not be interpreted as rejecting the zone of privacy notion with respect to disclosure.

1851. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

1852. *See* Barrett, *Personal Rights, Property Rights and the Fourth Amendment*, 1960 SUP. CT. REV. 46.

1853. *See* United States v. United States District Court, 407 U.S. 297, 323 (1972); Chimel v. California, 395 U.S. 752, 762-64 (1969).

1854. *See* Camara v. Municipal Court, 387 U.S. 523 (1967).

related to governmental purposes and functions."[1855] Under this test, census questionnaires have been sustained,[1856] despite the wide scope of census questions.[1857] Moreover, witnesses subpoened by grand juries cannot challenge information requests by alleging that the grand jury lacked any reasonable ground for suspecting any criminal violations,[1858] nor can they object to questions on relevance grounds.[1859] In sum, fourth amendment privacy poses at most a minor barrier to government collection of information from the population at large.

A line of cases beginning in the 1950's suggests that the first amendment is a source of a right of disclosural privacy.[1860] Many of these cases involved legislative investigations conducted by the House Un-American Activities Committee, or by similarly purposed state committees. The controversies arose when witnesses before the committees refused to answer questions concerning the association of other individuals with the Communist Party on the basis that the first amendment barred the committee from forcing such disclosure.[1861] The Court concluded that "privacy of association" was a necessary concomitant to first amendment freedoms, that forced disclosure would abridge those freedoms, and that to justify such an abridgement a state must "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest."[1862] Other related cases have similarly made clear that a state's power to make inquiries about a person's beliefs or associations is limited by the first amendment.[1863] In the areas of public employment[1864] and bar admission[1865] in particular the Court has disallowed broad sweeping inquiries for purposes of determining

1855. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

1856. *See* United States v. Rickenbacker, 309 F.2d 462, 463 (2d Cir. 1962), *cert. denied*, 371 U.S. 962 (1963).

1857. *See* text at notes 1925-38 *infra*; notes 1990-93 *infra* and accompanying text.

1858. Hale v. Henkel, 201 U.S. 43 (1906); Levinson v. Attorney General, 321 F. Supp. 984 (E.D. Pa. 1970). *See generally* United States v. Calandra, 414 U.S. 338 (1974); Branzburg v. Hayes, 408 U.S. 665 (1972).

1859. Blair v. United States, 250 U.S. 273 (1919). *See also* United States v. Girgenti, 197 F.2d 218 (3d Cir. 1952).

1860. *See, e.g.*, Barenblatt v. United States, 360 U.S. 109 (1959). *See also* Shelton v. Tucker, 364 U.S. 479 (1960); NAACP v. Alabama, 357 U.S. 449 (1958).

1861. The issue in these cases was not whether the committees had the inherent investigative power to require answers but whether the Bill of Rights served as a limitation on the inherent investigative power. *See, e.g.*, Barenblatt v. United States, 360 U.S. 109, 114 n.2 (1959); Uphaus v. Wyman, 360 U.S. 72, 75 (1959).

1862. Gibson v. Florida Legislative Investigation Commn., 372 U.S. 539, 546 (1962).

1863. *See, e.g.*, Baird v. State Bar, 401 U.S. 1, 6 (1971).

1864. *See, e.g.*, Keyshian v. Board of Regents, 385 U.S. 589 (1967); Elfbrandt v. Russell, 384 U.S. 11 (1966); Shelton v. Tucker, 364 U.S. 479 (1960).

1865. *See, e.g.*, *In re* Stolar, 401 U.S. 23 (1971); Baird v. State Bar of Arizona, 401 U.S. 1 (1971).

fitness that discourage the exercise of first amendment rights. Thus, although these cases have focused on the "chilling effect" that disclosure would have on the exercise of first amendment freedoms,[1866] they clearly hold that the first amendment protects disclosural privacy interests and lend at least some support for the construction of a right of disclosural privacy.

There are, however, two limitations on the general rule that governments cannot violate constitutional rights when acquiring information[1867] that may restrict an individual's ability to assert a first amendment privacy right as a defense to a governmental demand for informaton. First, recipients of information requests generally are unable to assert by way of defense violations of the constitutional rights of third parties,[1868] at least where no injury in fact is demonstrated by the recipient.[1869] This bar on the assertion of constitutional *jus tertii* has many exceptions, however, and in recent years it has been honored mostly in the breach.[1870] Thus, in *NAACP v. Alabama*[1871] the NAACP was allowed to assert the first amendment rights of its members in response to a state request for its membership list. Similarly, in *Griswold v. Connecticut*[1872] a doctor and a birth control official were permitted to assert the privacy rights of the recipients of contraceptives as a defense to criminal charges of aiding and abetting the use of birth control devices. Second, as pointed out in *Eastland v. United States Servicemen's Fund*,[1873] the speech and debate clause limits the ability to raise constitutional defenses in response to requests for information from members of Congress or their aides. In *Eastland*, the plaintiff organization sought to enjoin implementation of a congressional subpoena *duces tecum* that directed a bank to produce the organization's bank records and alleged that compliance with the subpoena would violate the organization's first amendment rights. Had the subpoena been issued directly to the organization, it could have resisted and tested the subpoena in a

1866. *But see* Gibson v. Florida Legislative Investigation Commn., 372 U.S. 539, 565, 570 (1963) (Douglas, J., concurring). *See also* Beaney, *supra* note 1830.

1867. *See* Watkins v. United States, 354 U.S. 178, 188 (1957). *See also* Barenblatt v. United States, 360 U.S. 109 (1959). It is interesting to note that the early cases, *e.g.*, McGrain v. Daugherty, 273 U.S. 135, 173 (1927); Kilbourn v. Thompson, 103 U.S. 168, 190 (1880), which limited the scope of the investigative power by inherent purpose and pertinency requirements rather than by the Bill of Rights, were motivated at least in part by a desire to protect a citizen's "private affairs."

1868. *See, e.g.*, Village of Belle Terre v. Boraas, 416 U.S. 1, 10-11 (1974) (Brennan, J., dissenting); Eisenstadt v. Baird, 405 U.S. 438, 443-46 (1972); Tileston v. Ullman, 318 U.S. 44 (1943) (per curiam).

1869. *See* Note, *Standing To Assert Constitutional Jus Tertii*, 88 HARV. L. REV. 423, 428-31 (1974).

1870. *See* Note, *supra* note 1869, at 423 n.3 (citing cases).

1871. 357 U.S. 449 (1958).

1872. 381 U.S. 479 (1965).

1873. 43 U.S.L.W. 4635 (U.S. May 27, 1975).

contempt proceeding.[1874] In this context, however, the speech and debate clause limited the scope of the inquiry to whether the congressional act was within the sphere of legislative activity.[1875] While significant, the restriction on the assertion of constitutional rights resulting from the speech and debate clause is of limited force: it arises only at the federal government level when information is requested of third parties by members of Congress or by congressional aides carrying out legislative tasks.[1876]

The final three possible constitutional bases for a right to privacy—the penumbras emanating from the first eight amendments, the ninth amendment, and the concept of ordered liberty guaranteed by the due process clauses of the fifth and fourteenth amendments—have been explored collectively in a series of cases dealing with the privacy of autonomy. In *Griswold v. Connecticut*,[1877] the Court struck down statutes prohibiting the prescription or use of contraceptives in so far as the statutes related to married couples. Six justices, in three opinions, found an independent right of privacy, although they could not agree on its source. Justice Douglas, writing for the Court, advanced the penumbra theory.[1878] He attempted to demonstrate that the Bill of Rights applies to the states through the due process clause of the fourteenth amendment and protects the right of marital privacy by arguing that the specific guarantees of the first eight amendments give rise to "peripheral rights"[1879] without which the specific rights would be less secure. Thus, he asserted that the first amendment, whose penumbra includes associational privacy, the third amendment, which prohibits quartering soldiers in any house in time of peace without the owners' consent, the fourth amendment, which protects against unreasonable search and seizure, and the fifth amendment, which protects the citizen against self-incrimination, when taken together give rise to "zones of privacy."[1880]

Rejecting the penumbra approach, Justice Harlan considered the right of privacy so fundamental that it was "implicit in the concept of ordered liberty" and hence protected by due process.[1881] Justice Harlan had previously advanced the fundamental rights ap-

1874. 43 U.S.L.W. at 4638 n.14, 4641 n.16.

1875. 43 U.S.L.W. at 4638.

1876. The concurring opinion in *Eastland* by Justices Marshall, Brennan, and Stewart suggested that the plaintiff organization could have raised its constitutional rights by employing a different procedure with different parties defendant: "Our prior cases arising under the Speech and Debate Clause indicate only that a Member of Congress or his aide may not be called upon to defend a subpoena against constitutional objection, and not that the objection will not be heard at all." 43 U.S.L.W. at 4643.

1877. 381 U.S. 479 (1965).

1878. 381 U.S. at 484.

1879. 381 U.S. at 483.

1880. 381 U.S. at 484.

1881. 381 U.S. at 500.

proach to privacy in *Poe v. Ullman*,[1882] where he stated that "it is not the particular enumeration of rights in the first eight Amendments which spell out the reach of Fourteenth Amendment due process, but rather . . . those concepts which are considered to embrace those rights 'which are . . . *fundamental*; which belong . . . to the citizens of all free governments.' "[1883] This approach apparently was also adopted by Justice Goldberg, even though he joined in the Court's opinion and stated that he was adding his own opinion merely to "emphasize the relevance of [the ninth] Amendment." Justice Goldberg argued that the ninth amendment "shows a belief of the Constitution's authors that fundamental rights exist that are not expressly enumerated in the first eight amendments and an intent that the list of rights included there not be deemed exhaustive."[1884] One must look, he stated, to the " 'traditions and [collective] conscience of our people to determine whether a principle is so rooted [there] . . . as to be ranked as fundamental.' "[1885] The right of privacy in Justice Goldberg's view was just such a fundamental personal right, which emanated "from the totality of the constitutional scheme under which we live."[1886]

The debate over the constitutional source of the right of privacy apparently was settled in *Roe v. Wade*,[1887] in which the Court upheld a woman's absolute right to have an abortion in the first trimester of pregnancy. This holding struck down a state statute making abortions illegal except where the mother's life is endangered.[1888] Adopting the fundamental rights approach, the Court held that the "right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state actions, as we feel it is, or, as the district court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to en-

---

1882. 367 U.S. 497, 539-45 (1961) (Harlan, J., dissenting).

1883. 367 U.S. at 497. Justice White, concurring in *Griswold*, also found justification in the liberty guaranteed by the fourteenth amendment, but he refused to recognize that this liberty gave rise to an independent right of privacy. *See* 381 U.S. at 502-07. Justices Black and Stewart dissented on the ground that the fourteenth amendment makes applicable to the states no rights beyond those specifically incorporated in the first ten amendments. *See* 381 U.S. at 507-31.

1884. 381 U.S. at 492.

1885. 381 U.S. at 493 (brackets in original), *quoting* Snyder v. Massachusetts, 291 U.S. 97, 105 (1934).

1886. 381 U.S. at 494, *quoting* Poe v. Ullman, 367 U.S. 497, 517 (1961) (Douglas, J., dissenting).

1887. 410 U.S. 113 (1973). *See also* Paris Adult Theatre I v. Slaton, 413 U.S. 49, 65 (1973).

1888. The Court did, however, reverse the district court's decision to the extent that it had held that this right of privacy was unqualified, holding instead that the state's interest in protecting the potentiality of human life in the second and third trimesters of pregnancy was sufficiently strong to permit some regulation of abortion. *See* 410 U.S. at 154.

compass a woman's decision whether or not to terminate her pregnancy."[1889] Because the plaintiff in *Roe v. Wade* was an unmarried woman,[1890] the holding affirms that the right of privacy attaches to the individual and is not restricted to the marital relationship. There are at least two reasons that may explain why the Court settled on the fundamental rights approach. First, the composition of the Court had changed drastically. Of the five justices who joined the majority in *Griswold*, only Justices Douglas and Brennan remained; additionally, both Justices Black and Harlan had departed. Second, the Court could have found the penumbra theory unmanageable because it opened up so much uncharted ground. The fundamental rights approach has been a traditional one[1891] and, because of the amorphous quality of the "liberty" concept, the approach is no less open to expansion than the penumbral argument.

One other Supreme Court case, *Stanley v. Georgia*,[1892] expanded the privacy concept to include the right to possess obscene materials in one's home. While the Court ostensibly based its holding on the first amendment, the decision drew in part upon a "fundamental . . . right to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy. "[1893] The privacy underpinning in *Stanley* was clearly significant, because the case is difficult to reconcile with other cases holding that the first amendment does not apply to obscenity,[1894] and because the right recognized in *Stanley* is limited to the house,[1895] unlike most first amendment

1889. 410 U.S. at 153.

1890. 410 U.S. at 120.

1891. As early as Meyer v. Nebraska, 262 U.S. 390 (1923), the Court recognized certain "fundamental" rights that would be protected despite their lack of explicit recognition in the Constitution. In subsequent cases, the Court recognized as fundamental rights included in the liberty clause of the fifth and fourteenth amendments the personal intimacies of the home, the family, procreation, motherhood, marriage, and child rearing. *Cf.* Eisenstadt v. Baird, 405 U.S. 438 (1972); Stanley v. Georgia, 394 U.S. 557 (1969); Loving v. Virginia, 388 U.S. 1 (1967); Griswold v. Connecticut, 381 U.S. 479 (1965); Skinner v. Oklahoma, 316 U.S. 535 (1942); Pierce v. Society of Sisters, 268 U.S. 510 (1925). *See also* Village of Belle Terre v. Boraas, 416 U.S. 1, 12 (1974) (Marshall, J., dissenting), in which Justice Marshall stated that the right of privacy should extend to the selection of living companions: "The choice of household companions—of whether a person's 'intellectual and emotional needs' are best met by living with family, friends, professional associates or others—involves deeply personal considerations as to the kind and quality of intimate relationships within the home. That decision surely falls within the ambit of the right to privacy protected by the Constitution." 416 U.S. at 16. If these rights apply to the states through the due process clause of the fourteenth amendment, one may also find a right of privacy either in that same clause or in the liberty clause of the fifth amendment applying to the federal government.

1892. 394 U.S. 557 (1969).

1893. 394 U.S. at 564.

1894. *See, e.g.*, Paris Adult Theatre I v. Slaton, 413 U.S. 49, 54 (1973); Miller v. California, 413 U.S. 15, 23-25 (1973); Kois v. Wisconsin, 408 U.S. 229, 230 (1972); Roth v. United States, 354 U.S. 476, 485 (1957).

1895. *See* 394 U.S. at 558.

rights. Moreover, the Court cited *Griswold* in addition to first amendment cases to support the proposition that "the right to receive information and ideas" is "fundamental to our free society."[1896] In short, the Court apparently relied on first amendment considerations to justify expanding the incipient privacy right.

The contours of the privacy right developed by these cases seem extraordinarily difficult to determine, for the activities it has been invoked to protect lack a clear interrelationship. The Court often speaks of privacy as if it were a single right, but it seems more accurate to conceive of privacy as that characteristic common to those individual actions that the Court has been willing to recognize as fundamental rights. Thus, the Court has stated that "only personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty,' . . . are included in this guarantee of personal privacy."[1897] It is clear that not all fundamental rights fall within the ambit of the privacy right, but an underpinning of strong privacy interests seems to enhance the possibility that a particular right will be deemed fundamental. The actions protected thus far in the name of privacy relate to the home,[1898] the family,[1899] and individual sexuality.[1900] The Court seems to be guided by its perception of activities that society views as private and that are thus not fit subjects for government regulation.[1901] But it is not at all clear what other actions popularly considered private will receive constitutional protection.[1902]

The above-discussed privacy cases involve autonomy, not disclosure. A right of disclosural privacy, however, can be derived from the fundamental privacy rights by analogy to the first amendment right of disclosural privacy: Disclosure of information relating to an individual's participation in particular activities may deter an individual from engaging in those activities. Where the activities have the status of fundamental rights, any such deterrent effect would be an impermissible "chill." But the disclosural privacy right derived

1896. 394 U.S. at 564.

1897. Roe v. Wade, 410 U.S. 113, 152 (1973).

1898. *See* Stanley v. Georgia, 394 U.S. 557 (1969). *See also* Village of Belle Terre v. Boraas, 416 U.S. 1, 12 (1974) (Marshall, J., dissenting).

1899. *See* Griswold v. Connecticut, 381 U.S. 479 (1965); State v. Elliott, 44 U.S.L.W. 2044 (N.M. Ct. App. July 9, 1975).

1900. *See* Eisenstadt v. Baird, 405 U.S. 438 (1972); Population Servs. Intl. v. Wilson, 44 U.S.L.W. 2033 (S.D.N.Y. July 2, 1975).

1901. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 174 (1973) (Rehnquist, J., dissenting).

1902. *See generally* Note, *The Constitutionality of Laws Forbidding Private Homosexual Conduct*, 72 MICH. L. REV. 1613 (1974); Note, *supra* note 1720.

A few state courts, interpreting the federal Constitution have extended the right of privacy to other areas. *See* Davidson v. Dill, 180 Colo. 123, 128, 503 P.2d 157, 161 (1972); Eddy v. Moore, 5 Wash. App. 334, —, 487 P.2d 211, 217-18 (1971) (arrest records); City of Carmel-by-the-Sea v. Young, 2 Cal. 3d 259, 266-68, 466 P.2d 225, 230-32, 85 Cal. Rptr. 1, 6-8 (1970) (financial disclosures by public officials).

from the privacy cases arguably should go beyond those situations in which a chilling effect can be shown. For example, requiring disclosure of the reasons why a woman decides to have an abortion may not deter the exercise of this fundamental right because the consequences of having an unwanted child are so enormous. Nevertheless, this information seems so private that the government should not in most instances be able to require its disclosure. The same high regard for privacy that led the Court to conclude that government regulation of abortions is improper, at least in the first trimester, should mandate disclosural privacy with regard to information concerning abortions in the first trimester. In situations where the state's regulatory purposes are outweighed by a concern for individual privacy, the state should be unable to investigate, even for a tangentially related purpose such as public health, without showing a very strong interest. Thus, with regard to information relating to contraception, the bearing and rearing of children, private obscenity, and any other activities recognized as fundamental privacy rights, it can be argued that there is a corresponding fundamental right of disclosural privacy, although no case to date has so held.[1903] While the right of disclosural privacy derived in this manner from fundamental rights would not be as broad as the disclosural privacy right inferred from the fourth amendment, its exceptions would be more restricted. A state infringement of fundamental rights can only be justified by a compelling state interest[1904] and the infringing legislation "must be narrowly drawn to express only the legitimate state interests at stake."[1905] Thus it seems possible to develop a right of disclosural privacy offering more protection than the broad but low walls of the fourth amendment.

1903. *But cf.* Roe v. Ingraham, 480 F.2d 102 (2d Cir.), *on remand*, 364 F. Supp. 536 (S.D.N.Y. 1973); Merriken v. Cressman, 364 F. Supp. 913 (E.D. Pa. 1973).

The Supreme Court bypassed an opportunity to discuss this issue in Roe v. Norton, 43 U.S.L.W. 4874 (U.S. June 24, 1975), which involved a challenge to a state statute providing criminal sanctions for mothers of illegitimate children receiving AFDC assistance who refused to divulge the name of the putative father of the child. A three-judge district court had upheld the statute against claims of denial of due process and equal protection and invasion of right to privacy, and the Supreme Court granted certiorari. The Social Security Act was amended in the interim, however, and the case was remanded for reconsideration in light of that development.

On the state level, the New York supreme court, in Schulman v. New York City Health & Hospitals Corp., 70 Misc. 2d 1093, 335 N.Y.S.2d 343 (1972), *vacated and remanded*, 41 App. Div. 2d 714, 341 N.Y.S.2d 242, *judgment reinstated*, 75 Misc. 2d 150, 346 N.Y.S.2d 920 (Sup. Ct. 1973), *revd.*, 44 App. Div. 2d 482, 355 N.Y.S.2d 781 (1974), found that a state law requiring disclosure of the name and address of abortion patients was void because it violated the patient's constitutional right to privacy. In reversing, the Appellate Division relied on its finding that there was "a sufficient compelling state interest . . . to justify limiting the fundamental right of privacy asserted . . . ." 44 App. Div. 2d at —, 355 N.Y.S.2d at 785. *See generally* Note, *supra* note 1720, at 770-72.

1904. Roe v. Wade, 410 U.S. 113, 155 (1973).

1905. Roe v. Wade, 410 U.S. 113, 155 (1973).

It would be somewhat misleading to treat disclosural privacy as a unitary right, because it is derived from dissimilar freedoms of action guaranteed by the first and fourth amendments and by the due process clauses of the fifth and fourteenth amendments. One particular distinction is that the disclosural privacies implied from the fundamental rights of autonomous privacy depend much more on a notion that disclosure would be offensive to societal norms than do the disclosural privacy rights inferred from the first amendment. In addition, first amendment disclosural rights require the demonstration of a chilling effect on the freedom of association or speech, while the other disclosural privacy rights arguably exist independent of any chilling effect. Nevertheless, the disclosural privacy rights probably have enough similarities to make it convenient to speak of them as one class of rights.

One principal similarity among the disclosural privacy rights is the standard the government must meet to justify an infringement. In all cases the state must show a compelling state interest,[1906] a very heavy burden. Even this standard has been viewed as a balancing test,[1907] however, and it is possible to argue that the individual's disclosural privacy interest is not entitled to as much weight as the individual's interest in exercising the underlying first or fourth amendment rights or privacy rights of autonomy. The individual's right to act is arguably more important than his right not to disclose what he does. For example, it seems more important to protect the decision whether to bear a child than to protect the woman's right to disclose that decision.

The application of this compelling state interest standard may yield results that are varying and difficult to predict. Because disclosural privacy rights are derived from other constitutional rights, the weight of each disclosural right may vary according to the weight of the underlying right. It has been maintained, for example, that the first amendment rights are entitled to a special degree of protection.[1908] On the other side, the force of the government's interest in

---

1906. Several state courts have found a compelling state interest sufficient to override the privacy right. *See* Atchison, T. & S.F. Ry. v. Lopez, — Kan. —, —, 531 P.2d 455, 467 (1975) (state's interest in preventing employment discrimination justified release of arrest and conviction records to state civil rights commission); Schulman v. New York City Health & Hospitals Corp., 44 App. Div. 2d 482, —, 355 N.Y.S.2d 782, 785 (1975) (state's interest in regulating abortions justified disclosure of abortion patient's name and address to Board of Health). *But see* Eddy v. Moore, 5 Wash. App. 334, —, 487 P.2d 211, 217-18 (1971) (state did not show a compelling state interest in retaining arrest records of acquitted persons).

1907. *Cf.* Note, *Reaffirming the Freedom of the Press: Another Look at* Miami Herald Publishing Co. v. Tornillo, 73 MICH. L. REV. 186, 199 (1974); Note, Salyer Land Co. v. Tulare Lake Basin Water Storage District: *Opening the Floodgates in Local Special Government Elections*, 72 MICH. L. REV. 837 (1974).

1908. *See* New York Times v. Sullivan, 376 U.S. 254, 269-72 (1964); West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624, 638-42 (1943); Whitney v. California, 274

disclosure may depend upon the source of the governmental investigative power being invoked. For example, the congressional investigative power implied from the impeachment function may present a stronger governmental interest than the investigative power implied from the legislative function. In an investigation under the impeachment function, the integrity of the institutions of government are involved, while in an investigation under the legislative function, only the ability to pass a specific piece of legislation is at stake. Although the legislative investigatory power is important, it is arguably less compelling than that implied from the impeachment function.

Even if courts are willing to recognize as extensive a disclosural privacy right as advocated above, there remains a need for legislative action if individuals are to be protected adequately from intrusive government information acquisition. One reason is that the balancing test gives little guidance concerning the proper limits of government intrusion into individual privacy, for the test leaves a judge free to apply his own value judgments in assessing competing state and individual interests in a particular case. A second reason is that because the right of disclosural privacy draws its strength from specific provisions of the Bill of Rights, it may be difficult to expand that right beyond matters relating to first amendment freedoms, sexual relations, the family, and the home. In any case, greater detail and flexibility in the protection of privacy interests can be accomplished legislatively. Moreover, a societal reassessment of conflicting interests is easier to implement when the original balance is struck legislatively than when the balance is accorded a constitutional dimension and is thus not within the legislature's power to change.

In addition to the need for legislative control of information acquisition, there is need for legislation in the areas of information retention and dissemination if the individual privacy interests at stake are to be adequately protected. The implications of the privacy right for these other aspects of information-handling are limited. In particular, simple retention of such information does not appear to represent any further infringement of the constitutional right. But in many instances, on a policy level, the government's desire to retain collected information indefinitely will not justify the resulting injury to individual privacy interests.

To be sure, in some areas the retention of information about an individual may continue to serve a purpose, at least as long as the individual is alive. Criminal conviction records, for example, are used as an important tool for sentencing after subsequent convictions.

U.S. 357, 373-78 (1927) (Brandeis, J., concurring); Abrams v. United States, 250 U.S. 616, 628-31 (1919) (Holmes & Brandeis, JJ., dissenting). *But see* Kovacs v. Cooper, 336 U.S. 77, 90-97 (1949) (Frankfurter, J., concurring).

Even where the purpose for which the information was collected can no longer be served, the government may nevertheless legitimately desire to retain the information in order to avoid the burden of having to recollect it, should it ever be needed again. The principal problem encountered with record retention is the possibility of disclosure, either intentional or inadvertent, to other persons or agencies of personal information traceable to specific individuals.[1909] This danger appeared so substantial to the court in *Menard v. Mitchell*[1910] that it viewed an order to expunge FBI records concerning an illegal arrest as a proper means of preventing inadvertent disclosure. The court stated that "if appellant can show that his arrest was not based on probable cause it is difficult to find constitutional justification for its memorialization in the FBI's criminal files,"[1911] especially because dissemination of that information might subject the appellant's reputation to substantial injury.[1912]

While legislation is needed, it is arguable that the right of disclosural privacy protects against the possibility that information may be accidentally revealed.[1913] If the government can assure confidentiality, there seems to be no constitutional requirement for disposal of information validly acquired. Moreover, dissemination by the collecting agency to other federal agencies of personally identifiable information would be permissible where the other agencies can show a need that is sufficiently compelling to justify collecting the information from the source itself. But, arguably, the right of disclosural privacy is violated unless each new governmental unit can satisfy such a test and unless the subject is given timely notice of any attempt at intra-governmental transfer: The agency from which the information is sought cannot be expected to assert satisfactorily the subject's rights. For the same reason, the collecting agency should have to make a new showing of need sufficient to justify collecting the in-

1909. *See, e.g.*, A. MILLER, *supra* note 1503. *But cf.* DATABANKS, *supra* note 1502. Proposals for a national data center have been criticized extensively because of confidentiality problems. *See, e.g.*, A. MILLER, *supra*; Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400 (1968); notes 2100-04 *infra* and accompanying text.

1910. 430 F.2d 486 (D.C. Cir. 1970). On remand, 328 F. Supp. 718 (D.D.C. 1971), however, the district court declined to order expungement and instead enjoined disclosure of the records to prospective employees other than agencies of the government. 328 F. Supp. at 728. On appeal from this district court refusal to expunge, the court of appeals remanded the case with orders "to remove appellant's record from [the] criminal files." Menard v. Saxbe, 498 F.2d 1017, 1030 (D.C. Cir. 1974). *See also* Tarlton v. Saxbe, 507 F.2d 1116 (D.C. Cir. 1974); United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1974).

1911. 430 F.2d at 492.

1912. On the problems of confidentiality in this context see Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968); Comment, *supra* note 1525.

1913. *But cf.* Eddy v. Moore, 5 Wash. App. —, —, 487 P.2d 211, 218 (1971); Davidson v. Dill, 180 Colo. 123, 128, 503 P.2d 157, 162 (1972).

formation before it can use the information for a new purpose. Finally, it is clear that dissemination to individuals or to private organizations without the consent of the person to whom the information pertains[1914] is unwarranted because private parties can never show the required compelling state interest or national governmental purpose.[1915]

D. *Federal Statutory Protection for Privacy Prior to the Privacy Act of 1974*

Prior to the Privacy Act of 1974, which is the first congressional effort at comprehensive privacy legislation, Congress attempted to reduce the damage to privacy caused by government data-handling through specific acts dealing with specific types of information. These enactments deal to varying degrees with all five critical problems of a data-gathering system: types of information that can be collected,[1916] methods of collection,[1917] retention,[1918] dissemination,[1919]

1914. But could an individual, in supplying the information to the government in the first place, be deemed to have consented to such dissemination? This is obviously not the case where the individual has objected to governmental collection in the first instance. But where the individual merely provides the requested information without objecting, the question becomes more difficult and depends upon the circumstances surrounding the initial disclosure. There is no reason to suppose that the ordinary common-law consent doctrine would not apply. Under this doctrine, consent may be either express or implied. Consent may be implied from silence only where a reasonable person would speak if he objected. Consent may also be inferred from custom or usage. Consent will be held invalid where it is obtained under situations of duress, where the threat is direct. The privilege is limited to the conduct to which the party actually consents, or to acts of a substantially similar nature. *See* W. PROSSER, *supra* note 1565, at 101-08. Yet one must consider that a governmental request for information may be inherently coercive. This has led Professor Miller to comment that "[E]ven a questionnaire sent out under the imprimatur of a federal agency has an intimidating effect on some people, a weakness that often is played upon by the agency in its follow-up practices." A. MILLER, *supra* note 1503, at 186.

1915. *But see* Tosh v. Buddies Supermarkets, Inc., 482 F.2d 329, 332 (5th Cir. 1973), holding that no right of privacy was invaded by the release of arrest records to nonlaw-enforcement persons for other than law enforcement purposes when those persons "present a legitimate need for and interest in the material."

1916. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. §§ 2511, 2516 (Supp. I 1971) (collection of information by interception of oral and wire communications); 28 U.S.C. § 534 (1970) (collection of criminal records by the federal government); 44 U.S.C. § 3505 (1970) (prohibiting federal agencies from collecting information that another agency has already been authorized to obtain); 44 U.S.C. § 3506 (1970) (determination as to the necessity of collection of information by a federal agency upon the objection of a party having a "substantial interest"); 44 U.S.C. § 3509 (1970) (requiring federal agencies to submit comprehensive plans for the collection of information); 44 U.S.C.A. § 3512 (Supp. Feb. 1975) (collection of information by independent regulatory agencies); 44 U.S.C. § 3511 (1970) (imposing penalties upon persons who fail to furnish requested information).

1917. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. §§ 2511, 2516, 2518 (Supp. I 1971) (permitting the collection of information by interception of wire or oral communications and outlining the authorization procedure for such interceptions); 44 U.S.C. § 3501 (1970) (requiring the minimization of the burden placed on persons compelled to furnish information to federal agencies); 44 U.S.C. § 3505 (1970) (prohibiting multiple collection of information by various agencies).

and remedies for a party injured by unlawful dissemination.[1920] Four major acts that exemplify the types of privacy protection Congress

---

1918. *See, e.g.*, 28 U.S.C. § 534 (1970) (retention of criminal identification records); Organized Crime Control Act of 1970 § 1001(a), 18 U.S.C. § 3578 (1970) (retention of criminal conviction records). The statutes regulating records-management by the Administrator of General Services are 44 U.S.C. § 2905 (1970) (establishing standards for the retention of records of continuing value); 44 U.S.C. § 2907 (1970) (establishing records storage centers); 44 U.S.C. § 2909 (1970) (allowing the Administrator to authorize the retention of records). The statutes regulating records-management by federal agencies are 44 U.S.C. §§ 3101-07 (1970). Regarding the disposal of records see 44 U.S.C. §§ 3301-14 (1970), especially section 3310, providing for the disposal of records constituting a menace to health, life, or property and section 3314, providing that the procedures for the disposal of records outlined in this chapter are to be exclusive.

1919. Numerous federal statutes regulate disclosures related to personal life. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-81t (1970); 18 U.S.C. § 1905 (1970) (disclosure of confidential information by government employees); 38 U.S.C. § 3301 (1970) (VA records); Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. § 2511 (1970) (general prohibition against disclosure of the contents of intercepted wire and oral communications); 42 U.S.C.A. § 1306 (1974) (disclosure of information in the possession of the Department of Health, Education, and Welfare and the Department of Labor); Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 § 333, 42 U.S.C. § 4582 (1970) (prohibiting the disclosure of the names of individuals who were the subjects of research on alcohol abuse); 28 U.S.C. § 534 (1970) (disclosure of criminal identification information); Organized Crime Control Act of 1970 § 1001(a), 18 U.S.C. § 3578 (1970) (disclosure of criminal conviction records); Postal Reorganization Act § 2, 39 U.S.C. § 410 (1970) (disclosure of information by the Post Office). Other statutes regulate the disclosure of financial and business records. *See, e.g.*, INT. REV. CODE OF 1954, § 6103 (disclosure of tax returns); Federal Trade Commission Act § 6(f), 15 U.S.C. § 46(f) (1970) (disclosure of trade secrets and names of customers); 7 U.S.C. § 608(d) (1970) (disclosure of information under the Agricultural Adjustment Act); Trust Indenture Act of 1939 § 321, 15 U.S.C. § 77uuu (1970) (disclosure of confidential information collected by the SEC). *See* GOVERNMENT DOSSIER, *supra* note 1511, at 26-29. However, provisions allowing the discretionary release of data by high ranking officials are common, thereby significantly lessening the assurance of limited access. *See, e.g.*, 13 U.S.C. § 8(a) (1970) (release of census data by Secretary of Commerce). Other data, the disclosure of which is not specifically restricted by statute, may be declared confidential and its disclosure limited pursuant to regulations promulgated under agency rule-making powers. *See, e.g.*, 32 C.F.R. §§ 1608.1-.17 (1974) (Selective Service System records); 15 C.F.R. §§ 30.90-.91 (1974) (import-export data held by the Census Bureau).

Several statutes regulate agency transfer of records. *See, e.g.*, 44 U.S.C. § 2906 (1970) (permitting the Administrator of General Services to inspect the records of any federal agency); 44 U.S.C. § 3507 (1970) (requiring agencies to cooperate with other agencies in making information available to each other); 44 U.S.C. § 3508 (1970) (limiting the types of information that may be disclosed by federal agencies).

1920. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. § 2520 (1970) (authorizing the recovery of civil damages, including punitive awards, if the interception of a wire or oral communication by a government official was unauthorized); Fair Credit Reporting Act §§ 616, 617, 15 U.S.C. §§ 1681n, 1681o (1970).

Many of these statutes contain sanctions against the violating party. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968 § 802, 18 U.S.C. § 2511 (1970) (criminal penalties for the violation of the disclosure provisions on the interception of wire and oral communications); 18 U.S.C. § 2518 (1970) (violations of the procedures specified for the interception of wire or oral communications can be punished by contempt and the suppression of evidence so obtained); 13 U.S.C. § 214 (1970) (penalties for wrongful disclosure of census data); INT. REV. CODE OF 1954, § 7213 (penalty for unlawful disclosure of tax returns); 44 U.S.C. § 3508 (1970) (penalties for the unlawful disclosure of information by federal agencies).

has employed are the provisions governing the census,[1921] the Omnibus Crime Control and Safe Streets Act of 1968,[1922] the Family Educational Rights and Privacy Act of 1974,[1923] and the Fair Credit Reporting Act.[1924] An analysis of these statutes reveals that the piecemeal approach to privacy protection has proved to be largely inadequate: None of these statutes provides protection for privacy interests at all stages of the information-handling cycle.

Congress has authorized the Census Bureau to collect information about agriculture,[1925] crime and delinquent classes,[1926] religious bodies,[1927] population, unemployment, and housing,[1928] and foreign commerce and trade.[1929] The authorizing legislation does not prevent the Bureau from obtaining information from any person or source it chooses. Indeed, it specifically permits the Secretary of Commerce to request other governmental offices or departments to provide data[1930] and to contract with educational and other research organizations for the preparation of monographs and other reports and materials of a similar nature.[1931] Collection of information by the Bureau is facilitated by sections providing for the imposition of criminal penalties upon persons refusing to answer questions or answering falsely and upon persons who fail to assist census employees in certain specified situations.[1932] Significantly, the authorizing legislation has no provisions specifying the methods to be used in collecting the information.[1933]

The statute allows the Bureau to use collected information only for statistical purposes[1934] and prohibits the publication of data that can be identified with a particular establishment or individual and the examination of individual reports by any nonemployee of the Bureau.[1935] The statute does provide, however, that the Secretary may disclose population, agriculture, and housing information for

1921. 13 U.S.C. §§ 1-307 (1970).

1922. Pub. L. No. 90-351, 82 Stat. 197 (codified in scattered sections of 5, 15, 18, 28, 42, 47 U.S.C.).

1923. 20 U.S.C.A. § 1232g (Supp. Feb. 1975).

1924. 15 U.S.C. §§ 1681-81t (1970).

1925. *See, e.g.*, 13 U.S.C. § 41 (1970) (cotton statistics); 13 U.S.C. § 61 (1970) (statistics on oilseeds, nuts, kernels, fats, oils, and greases).

1926. *See, e.g.*, 13 U.S.C. § 101 (1970).

1927. *See, e.g.*, 13 U.S.C. § 102 (1970).

1928. *See* 13 U.S.C. § 141 (1970) (permitting a decennial census).

1929. *See* 13 U.S.C. § 301 (1970).

1930. 13 U.S.C. § 6 (1970).

1931. 13 U.S.C. § 13 (1970).

1932. *See* 13 U.S.C. §§ 221-25 (1970).

1933. *But see* 44 U.S.C. §§ 3501, 3503-05 (1970) (applying to all federal agencies).

1934. 13 U.S.C. § 9 (1970).

1935. 13 U.S.C. § 9 (1970). This section does not, however, apply to information obtained from public records.

"genealogical and other proper purposes" to anyone requesting such information,[1936] with the sole stipulation being that such information may not be used "to the detriment of" people to whom the information relates.[1937] The sole remedy provided for wrongful disclosure of information is the imposition of criminal penalties upon the disclosing employee:[1938] no provision is made for compensating the party injured by the disclosure.

The Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973,[1939] includes numerous provisions regulating what information may be collected and what methods may be used in criminal investigations.[1940] The Act prohibits the use of illegally intercepted wire or oral communications,[1941] and requires that law enforcement research and statistical information identifiable to a particular person not be used for any purpose other than that for which it was obtained, that such information be immune from legal process, and that such information not be used as evidence or for any other purpose in any proceeding without the consent of the person furnishing the information.[1942] It further requires procedures to keep stored information current and to assure that the security and privacy of the information is protected, and entitles an individual who believes that criminal-history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of the Act, to review and obtain a copy of such information for purposes of challenge or correction.[1943] The Act imposes criminal fines on those violating the section on law enforcement research and statistical information,[1944] and fines or imprisonment on those willfully violating the provisions on wire and oral communications.[1945] The Act also allows for the recovery of civil damages by a person whose wire or oral communi-

---

1936. 13 U.S.C. § 8(a) (1970).

1937. 13 U.S.C. § 8(c) (1970). A number of state court decisions define "detriment," although no clear consensus emerges from these cases. *See, e.g.*, Supervisors of County of Boone v. Village of Rainbow Gardens, 14 Ill. 2d 504, 153 N.E.2d 16 (1958); State *ex rel.* Pritchard v. Board of Health, 198 S.2d 490 (La. Ct. App. 1967); State *ex rel.* Lytell v. Board of Health, 153 S.2d 498 (La. Ct. App. 1963); Stahl v. Board of Fin., 62 N.J. Super. 562, 163 A.2d 396 (1960); Wilkins v. City of New York, 25 Misc. 2d 27, 207 N.Y.S.2d 11 (Sup. Ct. 1960); Edwards v. Edwards, 239 S.C. 85, 121 S.E.2d 432 (1961).

1938. 13 U.S.C. § 214 (1970).

1939. Pub. L. No. 93-83, 87 Stat. 197 (codified in scattered sections of 5, 40, 42 U.S.C.).

1940. *See, e.g.*, 18 U.S.C. §§ 2510-20 (Supp. I 1971).

1941. 18 U.S.C. § 2511 (1970).

1942. 42 U.S.C. § 3771(a) (Supp. III 1973).

1943. 42 U.S.C. § 3771(b) (Supp. III 1973).

1944. 42 U.S.C. § 3771(c) (Supp. III 1973).

1945. 18 U.S.C. § 2511(1) (1970).

cations are unlawfully intercepted, including punitive damages and attorney's fees.[1946]

The final two statutes limit information gathering by federally regulated private and state institutions rather than by the federal government. They are nevertheless germane to the subject of limitations on the federal government's power to collect and keep personal data because they indicate congressional concern for individual privacy and include some particularly strong safeguards.

The Family Educational Rights and Privacy Act of 1974 (Education Act), applicable to all schools receiving federal funds, deals with the retention and dissemination of school-related information. It provides that students over the age of eighteen or attending "an institution of postsecondary education" and parents of all other students[1947] are to have the "right to inspect and review any and all official records, files and data directly related" to the students that are "intended for school use or to be available to parties outside the school or school system."[1948] The Act further provides that there shall be an "opportunity for a hearing to challenge the content of [the] . . . school records, to insure that the records are not inaccurate, misleading or otherwise in violation of the privacy or other rights of students . . . ."[1949] The Act prohibits the release of "personally identifiable records" without the consent of a student over eighteen or at a post-secondary educational institution, or of the parents of students under 18 except under limited circumstances.[1950] Where release of information is permitted to a third party, that party may not further disseminate the information without the consent of the parents or the student.[1951] The Act also requires that the parents or students be informed of the rights accorded them under it.[1952] Violation of the provisions of the Act results in the termination of federal funding to the violating institution.[1953]

The purpose of the Fair Credit Reporting Act (Credit Act),[1954] which applies to purely private organizations, is to ensure "that the

1946. 18 U.S.C. § 2520 (1970). The section provides a complete defense, however, for the good faith reliance on a court order and for actions taken in certain emergency situations.

1947. 20 U.S.C.A. § 1232g(d) (Supp. Feb. 1975).

1948. 20 U.S.C.A. § 1232g(a)(1) (Supp. Feb. 1975).

1949. 20 U.S.C.A. § 1232g(a)(2) (Supp. Feb. 1975).

1950. 20 U.S.C.A. § 1232g(b) (Supp. Feb. 1975).

1951. 20 U.S.C.A. § 1232g(b)(4)(B) (Supp. Feb. 1975).

1952. 20 U.S.C.A. § 1232g(e) (Supp. Feb. 1975).

1953. 20 U.S.C.A. §§ 1232g(a), (b), (c) (Supp. Feb. 1975).

1954. *See generally* Note, *The Fair Credit Reporting Act*, 56 MINN. L. REV. 819 (1972); Comment, *The Fair Credit Reporting Act: Are Business Credit Reports Regulated?*, 1971 DUKE L.J. 1229; Comment, *The Impact of the Fair Credit Reporting Act*, 50 N.C. L. REV. 852 (1972).

63-619 O - 76 - 85

consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information . . . ."[1955] The Credit Act does not contain any provisions limiting the scope of information that may be collected. It does, however, provide that the consumer must be informed that a report is being prepared about him, and requires advance notice and other special measures of protection where a report will involve interviews with friends and others concerning the subject's personal life.[1956] The bulk of the Credit Act relates to the retention and dissemination of information. It requires agencies to follow reasonable procedures to assure the maximum possible accuracy of the information they report,[1957] and like the Education Act, grants the consumer the right to learn what is in his file.[1958] The Credit Act also requires that obsolete information be removed from consumer reports[1959] and that challenged information be reported with a statement of the consumer's side of the dispute.[1960] Section 604 requires the consumer's permission before a credit reporting bureau may furnish any person with a credit report concerning him, except for a few specified purposes.[1961] Notwithstanding this provision, however, certain information may be provided to governmental agencies.[1962] An aggrieved person can recover actual damages and attorney fees for negligent noncompliance with the Act[1963] and punitive damages as well for willful noncompliance.[1964] The Act also imposes criminal penalties on officers or employees of a consumer reporting agency who knowingly and willfully disclose information concerning an individual to a person not authorized to receive that information.[1965]

All four of these acts provide at least some degree of protection for individual privacy interests. However, none is comprehensive. Of the four, none constitutes a real limitation on information acquisition: the Census provisions and Education Act place no restrictions on acquisition, the Crime Act prohibits only certain interceptions of oral and wire communications, and the Credit Act limits only

1955. Fair Credit Reporting Act § 602, 15 U.S.C. § 1681b (1970).
1956. Fair Credit Reporting Act § 606, 15 U.S.C. § 1681d (1970).
1957. Fair Credit Reporting Act § 607(b), 15 U.S.C. § 1681e(b) (1970).
1958. Fair Credit Reporting Act § 609, 15 U.S.C. § 1681g (1970).
1959. Fair Credit Reporting Act § 605, 15 U.S.C. § 1681c (1970).
1960. Fair Credit Reporting Act § 611, 15 U.S.C. § 1681i (1970).
1961. 15 U.S.C. § 1681b (1970).
1962. Fair Credit Reporting Act § 608, 15 U.S.C. § 1681f (1970).
1963. Fair Credit Reporting Act § 617, 15 U.S.C. § 1681o (1970).
1964. Fair Credit Reporting Act § 616, 15 U.S.C. § 1681n (1970).
1965. Fair Credit Reporting Act § 620, 15 U.S.C. § 1681r (1970).

interviews with friends and others concerning the personal life of the subject of a credit report. At the retention stage, all of the acts except the Census provisions have significant restraints on government information-handling, including provisions for subject access and challenge. In particular, the Crime and Credit Acts place affirmative duties on agencies to ensure that records are kept current. In the area of dissemination, all four of the acts apply: the Education and Credit Acts severely limit disclosure without the consent of the subject, the Crime Act allows most information to be used only for the purpose for which it was obtained, and the Census provisions, while allowing dissemination for proper purposes, proscribe the use of such information to the detriment of the subject. Finally, by way of remedies for the injured party, the acts are largely silent. The Credit Act apparently allows full recovery for negligent noncompliance with its provisions, but the Census and Education provisions have neglected the issue and the Crime Act allows recovery only for unlawful interceptions of wire and oral communications. Taken together, these acts demonstrate that a comprehensive privacy act was needed both to assure protection at all stages of the government's information-handling process, and to make the various privacy protections applicable to a much wider range of information-handling settings.

E. *The Privacy Act of 1974*

The Privacy Act of 1974 (Privacy Act)[1966] attempts to protect individual privacy interests by restricting the information practices of federal agencies.[1967] Although the Privacy Act deals with all stages

---

1966. 5 U.S.C.A. § 552a (Supp. Feb. 1975). The Senate bill, S. 3418, 93d Cong., 2d Sess. (1974), differed in several ways from the House bill, H.R. 16373, 93d Cong., 2d Sess. (1974). No conference report was prepared. For a comparison of the Senate and House versions and the compromises reached see *Analysis of House and Senate Compromise Amendments to the Federal Privacy Act, in* 120 CONG. REC. H12,243-46 (daily ed. Dec. 18, 1974).

The provisions of the Privacy Act that directly limit the acquisition, retention and dissemination of information and that grant the rights of subject notice, access, and challenge do not go into effect until 270 days following the day of enactment. Privacy Act § 8, 5 U.S.C.A. § 552a (note) (Supp. Feb. 1975).

1967. The Privacy Act relies on the definition of agency provided in section 552(e) of the FOIA. Privacy Act § 3, 5 U.S.C.A. § 552(a)(1) (Supp. Feb. 1975). For a discussion of that definition see text at notes 334-64 *supra*.

S. 3418, 93d Cong., 2d Sess. (1974), as originally proposed, would have regulated all information systems. Proponents of this approach pointed to the proliferation of private information systems, examples of invasions of privacy by nongovernmental organizations, and the need for a comprehensive approach to the problem. *Joint Hearings*, *supra* note 1641, at 161 (testimony of H. Eastman, representing the ACLU). *See also id.* at 242 (statement of D. McGraw, Assistant Commissioner of Administration, Minnesota). However, other witnesses argued that the first privacy legislation should be limited to regulating the information systems of the federal government. For example the National Retail Merchants Association thought the "risks to personal privacy created by governmental, as compared to private personal data systems" were sufficient

of the information-handling process, it primarily addresses the problems of subject access and dissemination. The Privacy Act requires publication of the existence and characteristics of all personal information systems kept by every federal agency,[1968] permits individuals[1969] to have access to records containing personal information about them,[1970] and requires the subject's consent to nonroutine transfers of such information.[1971] The Privacy Act also imposes criminal penalties[1972] and provides for civil remedies.[1973] As a whole, the Act adopts a broad formulation of the right of privacy, which protects the individual's interest in controlling the dissemination of the details of his identity.

In the hearings on the Privacy Act, many agencies argued that the adoption of a broad privacy concept would prevent proper agency administration[1974] and prove unduly expensive.[1975] Privacy advocates questioned these assertions in some instances,[1976] but urged

---

to warrant different legislation. *Id.* at 629. Professor Westin warned that a national registry of all data banks, including political, racial, religious, and ideological groups, might threaten first amendment rights. *Id.* at 71.

It seems wise that Congress limited the Privacy Act's coverage to federal agencies. The coalition of business, agencies, and state governments opposing extension of the Act could have defeated any broad privacy bill, crippled it, or delayed its passage for a long time. An act regulating federal information systems allows private organizations to regulate themselves voluntarily. It also provides a precedent for later privacy legislation, if needed.

1968. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(4) (Supp. Feb. 1975), set out in note 2052 *infra.*

1969. The Act defines "individual" as a "citizen of the United States or an alien lawfully admitted for permanent residence." Privacy Act § 3, 5 U.S.C.A. § 552a(a)(2) (Supp. Feb. 1975). It was argued in the hearings that privacy is an individual right and that corporate and individual interests should be protected in separate legislation. *See Access to Records, Hearings on H.R. 12206 Before a Subcomm. of the House Comm. on Government Operations*, 93d Cong., 2d Sess. 180 (statement of T. McFee, Deputy Assistant Secretary for Management Planning of Technology, HEW), 207 (statement of Representative Abzug) (1974) [hereinafter *Hearings on Access*]. *But see id.* at 207 (statement of Representative Koch).

1970. *See* text at notes 2055-69 *infra.*

1971. *See* text at notes 2107-23 *infra.*

1972. *See* text at notes 2154-56 *infra.*

1973. *See* text at notes 2129-53 *infra.*

1974. For example, the spokesperson for the VA testified, "It is considered appropriate to observe that the provisions of the bill could materially interfere with the agency's performance of its mission in ways other than increased administrative work load." *Hearings on Records, supra* note 1517, at 131. *See also id.* at 89 (statement of H. Peterson, Assistant Attorney General, Criminal Division, Department of Justice), 109 (statement of D. Cooke, Deputy Assistant Secretary of Defense).

1975. *See id.* at 62 (Civil Service Commission), 89 (Justice Department), 109 (Defense Department), 132 (VA).

1976. The General Services Administration permits individual access to records and the Deputy Assistant Secretary testified that the provision was not an undue burden on administration. *Id.* at 129. Moreover, experience with the access requirements of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-81t (1970), has shown that credit agencies have not been overburdened by requests for access. *Hearings on Access, supra* note

that in any case the nation should accept any unavoidable costs of ensuring privacy.[1977] The final bill thus represented a compromise between these interests.[1978] In several respects, however, the compromises made to secure passage of the Act unwisely diluted privacy protection. First, the Act fails to establish an adequate standard for restricting data acquisition.[1979] Second, it almost completely ignores the need to regulate methods of data-gathering.[1980] Third, although the Act provides significant protection during the retention stage,[1981] in several respects it severely restricts the right of subject access.[1982] Fourth, agencies can too easily evade the general requirement that an agency disseminate information about an individual only with his consent.[1983] Fifth, the provision establishing a civil cause of action for those injured by violations of the Act is ambiguous and could be interpreted to limit severely the instances in which this remedy is available.[1984] Sixth, the exemptions to the Privacy Act could be drawn more narrowly without interfering with important government functions.[1985] Finally, the provisions integrating the Privacy Act with the FOIA are ambiguous and could result in startling amendments to the FOIA.[1986] This section examines the deficiencies and interpretative difficulties in the provisions of the Privacy Act relating to each of these problem areas.

1. *Acquisition*

The Privacy Act authorizes each agency to collect[1987] "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[1988] The "relevant and necessary" standard,[1989] however, does little to limit government collection

---

1969, at 264-65 (testimony of S. Feldman, Assistant Director for Special Statutes, Bureau of Consumer Protection).

1977. *See* 120 Cong. Rec. H2462 (daily ed. April 2, 1974). The Office of Management and Budget was unable to provide an accurate cost estimate of the administration of the Privacy Act. S. Rep. No. 93-1183, 93d Cong., 2d Sess. 85 (1974).

1978. *See* 11 Weekly Comp. of Pres. Docs. 7 (Jan. 1, 1975).

1979. *See* text at notes 1987-2019 *infra*.

1980. *See* text at notes 2020-51 *infra*.

1981. *See* text at notes 2052-54 *infra*.

1982. *See* text at notes 2055-88 *infra*.

1983. *See* text at notes 2107-23 *infra*.

1984. *See* text at notes 2129-38 *infra*.

1985. *See* text at notes 2163-95 *infra*.

1986. *See* text at notes 2196-211 *infra*.

1987. The actual word used by the Privacy Act is "maintain," defined as including "maintain, collect, use, or disseminate." Privacy Act § 3, 5 U.S.C.A. § 552a(a)(3) (Supp. Feb. 1975).

1988. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(1) (Supp. Feb. 1975).

1989. Some members of Congress had opposed any limits on acquisition because

of data, as evidenced by questionnaires propounded in recent years by agencies that have long operated under similar standards. For example, Bureau of the Census guidelines for census questions include both relevance and need requirements.[1990] Nevertheless, the list of questions proposed for the decennial census of 1970, which engendered considerable controversy, included questions on religious affiliation, social security numbers, physical and mental handicaps, registration and voting records,[1991] smoking, moonlighting, union membership, and household pets.[1992] It also included questions on rent paid, value of houses owned, earnings, airconditioning, plumbing facilities, number of divorces, and the number of babies women had had.[1993] A much-criticized federal questionnaire, the Longitudinal Retirement History Survey[1994] issued under the aegis of the Census Bureau at the request of the Department of Health, Educa-

---

they doubted that a standard could be found that would give individuals some protection without also preventing agencies from carrying out their functions. *Cf. Hearings on Access*, *supra* note 1969, at 97 (statement of Representative Koch). They also thought that such a restriction was not necessary because a right of subject access could be used to discover and expose to Congress any agency excesses. *Id.* These arguments, however, fail to recognize that mere collection of data may produce psychological harm, *see* text at notes 1536-40 *supra*, or a "chilling effect" on the exercise of first amendment rights. *See* text at notes 1541-49 *supra*; *Hearings on Access*, *supra*, at 119-34. Moreover, reliance on congressional oversight is unrealistic. First, an individual may be unwilling to disclose to his elected representatives activities that might be considered un-American or unnatural. Second, it may be difficult to gain the attention of Congress, and, third, even if the individual is heard, Congress may not take any remedial action. *See also* STAFF OF THE SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 1ST SESS., REPORT ON MILITARY SURVEILLANCE OF CIVILIAN POLITICS 7 (Comm. Print 1973) [hereinafter MILITARY SURVEILLANCE OF CIVILIAN POLITICS]. Finally, congressional oversight is necessarily an ad hoc approach. A general standard allows resolution of many problems before they arise.

At the hearings on the Privacy Act, witnesses proposed a variety of alternatives to the relevant and necessary standard for limiting government-information acquisition. At one extreme, the director of the ACLU argued that there are some questions that cannot be justified on the basis of government need. *Hearings on the Census*, *supra* note 1509, at 270-78. At the other extreme, the standard of "relevant to a valid governmental function" was suggested. *Id.* at 106 (testimony of A. Miller, National Law Center, George Washington University). Intermediate suggestions included "a clear[ly] demonstrated need for the data," *id.* at 186 (testimony of A. Miller, Professor, University of Michigan Law School), and "reasonably necessary to a governmental purpose or for significant public information." *Id.* at 225 (letter from C. Fried, Professor, Harvard Law School).

1990. *Hearings on the Census*, *supra* note 1509, at 238.

1991. SUMMARY AND CONCLUSIONS, *supra* note 1515, at 12.

1992. A. MILLER, *supra* note 1503, at 135.

1993. *Hearings on the Census*, *supra* note 1509, at 153. After congressional hearings, the Bureau of the Census omitted the questions in the first list but not those in the second. *Id. passim. Cf. Hearings on the 1970 Census Questions Before the Subcomm. on the Census and Statistics of the House Comm. on the Post Office and Civil Service*, 89th Cong., 2d Sess. (1966) [hereinafter *Hearings on the 1970 Census Questions*].

1994. The questionnaire is reprinted in *Hearings on the Census*, *supra* note 1509, at 883-924.

tion, and Welfare,[1995] asked questions such as: "taking things altogether, would you say you are very happy, pretty happy, or not too happy these days,"[1996] "do you have any artificial dentures,"[1997] "what were you doing most of last week,"[1998] "do you or your spouse see or telephone your parents as often as once a week,"[1999] "what is the total number of gifts that you give to individuals per year."[2000] These questions were defended as relevant and necessary for legitimate governmental purposes.[2001] Similarly, agencies have defended a real estate survey asking for details about recent property acquisitions, including character of the property, price paid, method of payment, and amount of mortgage,[2002] and a Department of Defense questionnaire, distributed to retired members of the military reserve, asking not only how much the veteran earned in the previous year but also how much other members of the family earned.[2003]

As demonstrated by the foregoing examples of government information demands, the elasticity of the "relevance" concept and the large number of conceivable governmental "needs" make them unsatisfactory standards for limiting acquistition. A more flexible balancing approach would seem more desirable because of its ability to reconcile the conflicting interests on a case-by-case basis. Such a balancing test should forbid the collection of information about any individual unless the collector-agency can show a clearly demonstrable need that outweighs the individual privacy interests and should require consideration of at least the following factors: First, consideration should be given to the sensitivity of the information sought. Information entitled to constitutional[2004] or common-law[2005] protec-

---

1995. *Id.* at 883.

1996. *Id.* at 897 (question 55).

1997. *Id.* at 901 (question 64b).

1998. *Id.* at 884 (question 1).

1999. *Id.* at 904 (question 75a).

2000. *Id.* at 907 (question 99a).

2001. *See id.* at 283-68 (testimony of W. Chartener, Assistant Secretary of Commerce for Economic Affairs).

2002. *Reprinted in id.* at 12-13.

2003. *Reprinted in id.* at 37-53.

Congressional hearings on federal questionnaires suggested that some questions had been included upon request by private organizations, *id.* at 188 (testimony of A. Miller, Professor, University of Michigan Law School), some were unnecessary because the information was already available, *id.* at 33, and some were included for no apparent reason. *Id.* at 57 (statement of Senator Ervin). Federal employees have probably been subjected to the most offensive information demands. They have been asked to disclose such personal matters as race, religion and national origin, political, social, and sexual activities, family assets, and personal feelings about religion, family, and sex. S. REP. No. 90-534, 90th Cong., 1st Sess. 7 (1967).

2004. *See* text at notes 1789-915 *supra.*

2005. *See* text at notes 1562-625 *supra.*

tion would be the most sensitive, followed by information generally regarded as private and hence not commonly divulged. Under this test, for example, an agency would have to demonstrate a greater need in order to justify acquisition of information concerning an individual's political affiliation, which is constitutionally protected,[2006] than it would to justify collection of an individual's name, age, and sex. Second, consideration should be given to the importance of the purpose for which the information is sought and the logical nexus between the information and that purpose. The IRS, for example, has a greater need for financial information than does the Bureau of Census; the Department of Defense has a greater need to inquire into the general personal background of a person being considered for certain sensitive positions than the Postal Service does to make broad-ranging inquiries prior to promotion of its employees. Similarly, the agency need for information from government benefit recipients and government employees is greater than the need for information from those merely being surveyed. Third, consideration should be given to the form in which the information is to be stored. If the information will not be kept in individually identifiable files there is little potential for harm and a lesser demonstration of need should suffice.[2007] Finally, consideration should be given to the intended length of retention and breadth of dissemination. As each increases, so does the danger of misuse.

The Privacy Act does subject government acquisition of information to strict requirements in one significant area. It provides in subsection (e)(7) that no agency shall collect information "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom [a] record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[2008] The provision, presumably a reaction to military and CIA surveillance of civilians,[2009] was designed to protect the preferred status of the

---

2006. *See* text at notes 1860-63 *supra*.

2007. Even where information is not stored in individually identifiable files there is reason to require a showing of need before data collection because of the potential psychological harm and chilling effect on the exercise of rights. *See* text at notes 1536-49 *supra*.

2008. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(7) (Supp. Feb. 1975).

2009. Congressional hearings conducted in 1974 revealed that military surveillance of civilian activities had originated in World War I and had been going on, in varying degrees of intensity, ever since. In the wake of the riots in urban areas and on college campuses in the 1960's, the Army expanded its intelligence system so that by 1970 it was monitoring virtually all political protest in America. It was estimated that the Army had files on over 100,000 civilians unaffiliated with the Armed Forces. STAFF OF THE SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 92D CONG., 2D SESS., ARMY SURVEILLANCE OF CIVILIANS: A DOCUMENTARY ANALYSIS 76 (Comm. Print 1974) [hereinafter ARMY SURVEILLANCE OF CIVILIANS]. The collection plans promulgated were broad and vague, resulting in the gathering of much irrele-

first amendment.[2010] It goes further than the Constitution, however, by not requiring the demonstration of a "chilling effect."[2011] Yet in two respects the provision is deficient. First, the provision should give similar protection to the other, equally critical facets of the right of disclosural privacy, such as information relating to sexual attitudes and conduct and to personal activities with those related by blood or marriage.[2012] Second, the exception to the provision allowing collection of information with individual consent fails to recognize the fact that in many contexts information requests are coercive. The Senate report on the rights of federal employees found that in the federal service and similar organizational situations an employer information request is equivalent to a command.[2013] Government benefit recipients are similarly situated. To ensure full protection for the underlying constitutional rights in these situations, the provision instead should have required a knowing and intelligent consent.[2014]

Subsection (e)(3) of the Privacy Act requires each agency collecting information to "inform each individual whom it asks to supply information [of] . . . (A) the authority . . . which authorizes the solicitation of the information and whether disclosure is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) [the uses that can be made of the information without his consent]; and (D) the effects on him, if any, of not providing all or any part of the requested information." The apparent purpose of this requirement is to provide the individual with sufficient information to make an intelligent decision whether to surrender information or to challenge the information

---

vant, incorrect, ambiguous, and useless information. MILITARY SURVEILLANCE OF CIVILIAN POLITICS, *supra* note 1989, at 6. Information was collected about financial affairs, sex lives, and psychiatric histories, often by covert means. ARMY SURVEILLANCE OF CIVILIANS, *supra*, at 96.

The investigating Senate subcommittee rejected arguments that the monitoring was reasonably related to the duty of the Army to protect against a possible re-occurrence of civil disorders, and found that "there is no question that military surveillance of civilian political activity is illegal, at least in the sense that it was not authorized by law. . . . [T]he subcommittee cannot imply the need for such domestic operations from the military's limited domestic mission." MILITARY SURVEILLANCE OF CIVILIAN POLITICS, *supra*, at 7. The report also concluded that the military's activities were in violation of the first amendment. *Id.* at 9.

2010. S. REP. No. 93-1183, *supra* note 1977, at 56.

2011. *See* text at note 1866 *supra*.

2012. *See* text at notes 1898-900 *supra*.

2013. S. REP. No. 90-534, *supra* note 2003, at 5.

2014. If the right to privacy were acknowledged as a constitutional one, it is arguable that a knowing and intelligent waiver would be mandated by the Constitution. *Cf.* Johnson v. Zerbst, 304 U.S. 458, 464 (1938). Because the Supreme Court has modified this standard with respect to some rights, *see, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 235 (1973), it is preferable that the statute incorporate the stricter standard.

request. Such knowledge is likely to increase participation in data-gathering, enhance the reliability of information provided, reduce public resentment and suspicion of government practices, and encourage the public to comment on agency policy.[2015] However, three additions to subsection (e)(3) would aid in more fully achieving these goals and would make the provision more consistent with the Act's broad concept of the privacy right.

Principally, when the person from whom the information is sought will be the subject of the file, the collecting agency should explain to that individual his right to challenge collection and the procedure for challenge, and his rights of access to the file for the purpose of ensuring its accuracy.[2016] Additionally, before an agency collects information about a data subject from third persons, the agency should be required to reveal to the subject the names of such third persons and the type of information to be sought from them, except in situations where the agency is justified in keeping the existence of the investigation secret from the data subject. When information is collected from third persons, the subject's right of access to the file is an inadequate privacy protection[2017] because without notice the subject will in most instances have little reason to suspect that the file exists. To be sure, information known to others is not protected by the common-law concept of privacy.[2018] But the statute's protection should extend to this aspect of data acquisition because people are more inclined to respond to government requests for information than individual requests,[2019] and because the government, by virtue of its size and resources, has a greater capacity to disseminate information about an individual than has any private person.

A further problem with subsection (e)(3) is that its notice provisions apply only when an agency collects information by asking the individual directly. Because the Privacy Act imposes almost no limitations on the methods an agency can use to gather information, an agency could in some circumvent notice requirements by gathering data from third parties or by utilizing covert procedures. One solution to this problem would be to require notice to the data subject unless notice would frustrate legitimate programs of covert surveillance. A better solution, discussed below, is to limit agency use of nondirect methods of data collection.

2015. *See Joint Hearings, supra* note 1641, at 2304-07 (report prepared by A. Bell for the Committee on Rulemaking and Public Information of the Administrative Conference of the United States).

2016. The rights of subject access and challenge are discussed in the text at notes 2055-98 *infra*.

2017. *See* text at notes 2049-51 *infra*.

2018. *See* text at notes 1586-87 *supra*.

2019. *See Hearings on the Census, supra* note 1509, at 194 (testimony of A. Miller, Professor, University of Michigan Law School), 215 (testimony of C. Fried, Professor, Harvard Law School).

2. *Methods of Data Collection*

The Privacy Act's sole restriction on methods of data acquisition is the requirement in subsection (e)(2) that agencies "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." The provision reflects the basic principle of fairness, advocated by the Senate's report on the Privacy Act, "that where government investigates a person, it should not depend on hearsay or 'hide under the eaves,' but inquire directly of the individual about matters personal to him or her."[2020] It also "supports the principle that an individual should to the greatest extent possible be in control of information about him which is given to the government."[2021] The provision thus disfavors acquisition from third parties or by covert means, although it recognizes implicitly that such methods may be necessary "for financial or logistical reasons or because of other statutory requirements."[2022] While the legislative history makes clear that minor financial or logistical concerns are not to outweigh privacy interests,[2023] it does not answer the critical questions of when it will not be "practicable" to collect from the subject and when subsection (e)(2) will be overridden by other statutes.

As originally introduced, the subsection (e)(2) "greatest extent practicable" requirement applied to all government information acquisitions. In order to meet agency objections based on the needs of certain civil and criminal law enforcement programs, the provision was limited to instances where the information sought could affect the receipt of direct benefits under a federal program.[2024] The limitation was a rather crude method, however, of satisfying the agency objections. For example, although criminal investigations are completely exempted from subsection (e)(2) by the general exemptions of subsection (j)(2),[2025] not all civil investigations are exempted. Thus, in a social security fraud investigation, which could lead to a denial of benefits, the agency presumably would be required to comply with subsection (e)(2). More significantly, the limitation as enacted exempts numerous informational studies that are not aimed at civil law enforcement and are not related to the granting or denying of benefits under federal programs.[2026] Rather

2020. S. REP. No. 93-1183, *supra* note 1977, at 47.

2021. 120 CONG. REC. H12,245 (daily ed. Dec. 18, 1974).

2022. *Id.*

2023. *See* S. REP. No. 93-1183, *supra* note 1977, at 48.

2024. *Id.* at 47.

2025. *See* text at note 2174 *infra*, arguing that such an exemption is unnecessary.

2026. Therefore, under the Privacy Act the sensitive information gathered in the Longitudinal Retirement History Survey, *see* text at notes 1994-2000 *supra*, could be

than carve out in rough fashion an exception to the requirements of subsection (e)(2), Congress should have established a general standard applicable to all information acquisition that would take into account the nature of the agency's activities and the importance of the state's need for the information, as well as considerations of practicability. A provision prohibiting the use of any method of information collection that is unreasonable would allow these factors to be taken into account. Such a standard would require a balancing of the nature of the agency's function and considerations of practicability against privacy interests.

A reasonableness standard for acquisition methods could also remedy another deficiency of the Privacy Act—its failure to give an agency any guidance as to what methods of collection it may use once it has determined that it must collect information directly from the data subject. Hearings on the use of mandatory questionnaires,[2027] lie detector[2028] and psychological[2029] tests, and military surveillance of civilians[2030] have reflected congressional concern for this problem but have failed to produce any legislative solutions. A standard of reasonableness would clearly preclude the use of any presently illegal or unauthorized acquisition methods. The reasonableness of otherwise legal and authorized methods should depend at least on the government interest served by collection of the information, the reliability of the method, the dangers posed by the method, the degree of control the method allows the subject to retain over the amount of information revealed, and the practicability of alternative methods available. Inclusion of the first factor allows the government to use otherwise unreasonable methods if it can demonstrate a sufficiently great need. The second factor requires consideration of the extent to which the proposed method will collect accurate information. The third factor accounts for the fact that some methods of acquisition, such as covert surveillance, are potentially more dangerous than others because of a greater likelihood of misuse or because of their

---

sought from persons other than the individual. The same possibility exists with regard to all other "informational" surveys.

2027. *Hearings on the Census, supra* note 1509.

2028. *Hearings on Privacy and the Rights of Federal Employees Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 89th Cong., 2d Sess. (1966) [hereinafter *Hearings on Federal Employees*]; *Hearings on the Use of Polygraphs by the Federal Government Before a Subcomm. of the House Comm. on Government Operations*, 88th Cong., 2d Sess., 89th Cong., 1st Sess. (1964-1965) [hereinafter *Hearings on Polygraphs*].

2029. *Hearings on Psychological Testing Procedures and the Rights of Federal Employees Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess. (1965) [hereinafter *Hearings on Psychological Testing*].

2030. *Military Surveillance Hearings on S. 2318 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974) [hereinafter *Hearings on Military Surveillance*].

potential psychological impact. The fourth factor requires consideration of the basic privacy issue—the extent to which the data subject retains control over the information flow. The final factor ensures that the least offensive method will be used unless rendered infeasible by financial or logistical circumstances.

Consideration of these factors would probably lead to the conclusion, for example, that the use of lie detector and psychological tests to measure suitability for employment or promotion is unreasonable. The lie detector's reliability is suspect because of its dependence on the physiology of the testee[2031] and because lie detector results are susceptible to conscious manipulation by the testee.[2032] Psychological tests have recently come under attack because of racial bias[2033] and because of the absence of objective scientific principles to guide in the construction and evaluation of such tests.[2034] Moreover, the persons evaluating test results often lack the expertise needed to make the results reliable.[2035] In addition, these testing methods are dangerous because repeated use may lead to conformity among employees,[2036] may inhibit the exercise of rights,[2037] and may even degrade the individual.[2038] Such tests necessarily lead to the unnecessary acquisition of sensitive information[2039] and thus infringe on the indi-

---

2031. H.R. REP. No. 89–198, 89th Cong., 1st Sess. 12 (1965).

2032. *Id.* at 12-13.

2033. *See* A. MILLER, *supra* note 1503, at 91-92. *See also Hearings on Special Inquiry on Invasions of Privacy Before a Subcomm. of the House Comm. on Government Operations*, 89th Cong., 1st Sess. 334 (1965) [hereinafter *House Special Inquiry*].

2034. *See Hearings on Psychological Testing*, *supra* note 2029, at 33 ("personality testing is closer to alchemy and other nonsciences than it is to the truth"), 43.

2035. *See* A. MILLER, *supra* note 1503, at 97-98. *Cf.* H.R. REP. No. 89–198, *supra* note 2031, at 2, 14.

2036. Herman, *Privacy, the Prospective Employee and Employment Testing: The Need To Restrict Polygraph Testing*, 47 WASH. L. REV. 73, 112 (1971).

2037. *Hearings on Federal Employees*, *supra* note 2028, at 221 (testimony of L. Speiser).

2038. Herman, *supra* note 2036, at 86.

2039. Though the questions asked in a polygraph examination vary with each examiner, the aim is always to cover a broad range of topics in search of "unusual responses." The questioner then delves into the "problem" area. *Hearings on Polygraphs*, *supra* note 2028, at 38. Consider the sample question in a proposed manual for adapting the polygraph to pre-employment screening:

> HAVE YOU EVER SUFFERED A NERVOUS BREAKDOWN?
>
> If so, when; cause and period of adjustment; frequency; hospitalized or not; family problems; mental maladjustment; service connected; mild or severe; unable to face reality; carries world's problems on his shoulders; criminal act or tendencies; claustrophobia; afraid of height; insecurity; failed in all endeavors; heavily in debt; amnesia; and others.

R. FERGUSON, THE POLYGRAPH IN PRIVATE INDUSTRY 133-35 (1966).

The questions asked on personality tests are often even more probing, inquiring into matters of physical conditions and bodily functions, religious beliefs, and attitudes toward sex and sexual behavior. For example, consider the following questions on the Minnesota Multiphasic Personality Inventory administered to Peace Corps volunteers (to be answered true or false):

17. My father was a good man.

vidual's control over what information he releases. Psychological tests in particular have been characterized as "tests that are designed to overbear the will of the individual . . . by reaching behind conscious articulation."[2040] Finally, there are less intrusive alternative methods of evaluating employees and job applicants,[2041] as evidenced by the fact that many governments and organizations do not find a need to resort to such tests.[2042] It is arguable that government interests in national security and the safety of government employees justify use of these tests in limited circumstances.[2043] However, in light of all the objectionable characteristics of these tests, it is doubtful that even these important government interests would make these methods reasonable in the context of employment and promotion.

Under this reasonableness of means test the use of mandatory questionnaires similarly would be unreasonable in many cases. The compulsion of responses under implicit or explicit threats of punishment or loss of employment deprives the respondent of any real choice not to answer, and hence of any control over the information he reveals. Congressional hearings on this method suggest that in most instances voluntary questionnaires present an adequate alternative,[2044] and various private research groups and states have succeeded in obtaining sufficient responses to voluntary questionnaires.[2045] In certain situations the importance of the government's need for the

---

18. I seldom have constipation.
19. My sex life is satisfactory.
27. Evil spirits possess me at times.
75. I get angry sometimes.
78. I like poetry.
290. I believe my sins are unpardonable.
387. I have had no difficulty holding my urine.

Hearings on Federal Employees, *supra* note 2028, at 5-6.

2040. Herman, *supra* note 2036, at 128. A few labor arbitration decisions have denied the admissibility of polygraph results, in part because of the invasion of privacy. *See, e.g.*, Town and Country Food Co., 39 Lab. Arb. 332, 335 (1962); Lag Drug Co., 39 Lab. Arb. 1121, 1123 (1962).

2041. For example, careful interviews, analysis of past job performance, aptitude tests, and simulated exercises. Herman, *supra* note 2036, at 87.

2042. *Cf.* A. MILLER, *supra* note 1503, at 93. Twelve states have made the use of polygraphs in the employment context illegal. Four states specifically apply the prohibition to governmental agencies. Herman, *supra* note 2036, at 97-98. In 1953, the AEC discontinued use of the polygraph because the marginal increase in security did not offset the costs in personnel recruitment and employee morale. H.R. REP. No. 89-198, *supra* note 2031, at 16.

The Guidelines for Testing and Selecting Minority Job Applicants prepared by the California State Fair Employment Commission practically prohibit the use of personality testing as a pre-employment screening device. *Id.* at 119-20. A representative of the CSC testified that his agency does not use personality tests in any personnel decisions because, "these tests are subject to distortion, either purposefully or otherwise. Therefore, the scores are undependable as a basis for employment decisions." *House Special Inquiry*, *supra* note 2033, at 37.

2043. *See* A. MILLER, *supra* note 1503, at 98.

2044. *See Hearings on the Census*, *supra* note 1509, at 219.

2045. *See id.* at 132-47 (testimony of Representative Betts).

information probably does justify use of mandatory questionnaires. For example, enumeration of the population is arguably of special importance because it is specifically required by the Constitution[2046] and because it must be accurate in order to serve as the basis for apportionment for representation.[2047] Therefore, responses to questions on the decennial census regarding enumeration could probably be made mandatory. An agency may also be justified in compelling government employees and those seeking employment, and persons seeking or currently obtaining government benefits, to answer relevant questions.[2048] However, the agency would not be justified in compelling answers to questions that do not bear on the granting of the job or benefit.

A general standard of reasonableness would not only cover all the methods problems ignored by the Privacy Act but would subsume the current subsection (e)(2) test. The probable result of employing such a standard would be to increase the number of instances in which direct collection from the individual is required. Direct collection accords the subject more control over the disclosure of information about himself than alternative methods of collection from third parties or by covert means. Recent experience casts doubt on the reliability of covert surveillance,[2049] and data collected from third parties is generally less likely to be reliable than data collected directly from the data subject.[2050] Moreover, covert methods pose the danger that irrelevant information will be collected because such methods are insufficiently selective[2051] and because the subject cannot object to the collection of particular data. Thus, the reasonableness test would require direct collection from the data subject unless the government can show that direct collection is not practicable or that the government need to use other methods is paramount.

3. *Retention*

An individual needs some control over information retained by the government in order to minimize the danger of invasions of his

---

2046. U.S. CONST., art. I, § 2. The Constitution does not, however, require that response to the census be mandatory.

2047. However, it is arguable that even this reason does not justify compelling response. The 1960 census was considered sufficiently accurate even though the census was not returned by or never reached 3 per cent of the population as a whole, and 16 per cent of young nonwhites in ghetto areas. *Hearings on the Census*, *supra* note 1509, at 295.

2048. It might be argued that answers to questions in these situations are not really compelled because the person could forgo the job or benefit rather than answer the questions. This argument overlooks the fact that such a choice may not be available to a welfare or social security recipient or to a person needing or "locked-into" a federal job. *See* note 1622 *supra*.

2049. *See* note 2009 *supra*.

2050. *Cf.* S. REP. No. 93-1183, *supra* note 1977, at 48.

2051. *See* note 2009 *supra*.

privacy. By giving the subject of a file the rights of notice, access, and challenge, the Privacy Act enables an individual to find out if an agency has collected information about him, what the information is, and how he can amend it.

The Privacy Act grants the right of notice in two provisions. Subsection (e)(4) requires each agency to publish in the *Federal Register* at least annually a notice of the existence and character of the systems of records it maintains that is sufficiently explicit to enable an individual to guess accurately which agencies maintain records about him.[2052] Subsection (f)(1) requires agencies to respond to individual inquiries as to whether the information systems named by the individual contain records pertaining to him. An individual can thus locate all federal records pertaining to him by first consulting the *Federal Register* and then writing to all the agencies that maintain the type of records likely to concern him. These provisions of the Privacy Act have been criticized on the ground that it is unrealistic to expect individuals to go to the trouble of writing to the agencies.[2053] However, requiring agencies to notify all persons about whom they presently maintain files would be inordinately expensive. Moreover, in the future each agency will have to notify file subjects when it collects information directly from them.[2054] The approach taken by the Privacy Act on this point thus appears to be a reasonable accommodation of privacy interests and the financial considerations of administration.

The creation of general rights of subject access and challenge is perhaps the most important contribution of the Privacy Act.[2055] Sub-

2052. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(4) (Supp. Feb. 1975), requires that each agency

> maintaining a system of records subject to the provisions of . . . this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records, which notice shall include—
>
> (A) the name and location of the system;
>
> (B) the categories of individuals on whom records are maintained in the system;
>
> (C) the categories of records maintained in the system;
>
> (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
>
> (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
>
> (F) the title and business address of the agency official who is responsible for the system of records;
>
> (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
>
> (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
>
> (I) the categories of sources of records in the system.

2053. *See Hearings on Records*, *supra* note 1517, at 52 (statement of Representative Mikva). *See also Hearings on Access*, *supra* note 1969, at 98 (statement of Representative Abzug).

2054. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(3) (Supp. Feb. 1975). *See* text following note 2014 *supra*.

2055. A 1974 survey of federal agency information practices revealed that only 53

section (d)(1) establishes a general right of subject access by requiring each agency to permit any individual, upon request, to review his record and obtain a copy of it.[2056] Such a right of access is the first step toward effective individual control over government information practices and is a necessary prerequisite to a right of challenge and to control over dissemination of the file. Furthermore, it enables individuals to discourage government collection of irrelevant information: When inspection reveals improper information in a file, the subject can publicize the agency's improper acquisition of data in order to put political pressure on the agency.[2057] Finally, the right of access enables the individual to obtain "the psychological sense of having satisfied oneself about what is really [in his file]."[2058]

Despite the broad language of this provision,[2059] it does not apply to the CIA,[2060] the Secret Service,[2061] and to criminal[2062] law enforcement agencies. Blanket exemptions for these agencies are examined below.[2063] The Act also exempts, without regard to the agency, the following six categories of information: classified information,[2064] statistical information,[2065] "examination material used solely to de-

---

per cent of the responding agencies permit an individual to review his or her entire file. *See* FEDERAL DATA BANKS, *supra* note 1515, at XLIII, LIII. The survey did not report on the rights of subject challenge. The FOIA, 5 U.S.C. § 552, *as amended*, 5 U.S.C.A. § 552 (Supp. Feb. 1975), allows access to some records, but gives no right of challenge.

2056. Privacy Act § 3, 5 U.S.C.A. § 552a(d) (Supp. Feb. 1975), provides:

> Access to Records.—Each agency that maintains a system of records shall—
>
> (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

Privacy Act § 3, 5 U.S.C.A. § 552a(c) (Supp. Feb. 1975), requires each agency both to keep an accounting of disseminations of records to other agencies, and to allow subject access to such accountings. Subsection (c) thus facilitates the right of access and challenge by enabling the subject to find his file no matter where it has been transferred.

2057. *Hearings on Access*, *supra* note 1969, at 97 (testimony of Representative Koch).

2058. S. REP. No. 93-1183, *supra* note 1977, at 60.

2059. The only restriction in the subsection itself is that "nothing in this section shall allow an individual access to information compiled in reasonable anticipation of a civil action or proceeding." Privacy Act § 3, 5 U.S.C.A. § 552a(d)(5) (Supp. Feb. 1975). This clause is meant to ensure that the Privacy Act does not alter the present rules of discovery. S. REP. No. 93-1183, *supra* note 1977, at 75.

2060. Privacy Act § 3, 5 U.S.C.A. § 552a(j)(1) (Supp. Feb. 1975).

2061. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(3) (Supp. Feb. 1975).

2062. Privacy Act § 3, 5 U.S.C.A. § 552a(j)(2) (Supp. Feb. 1975).

2063. *See* text at notes 2163-82 *infra*.

2064. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(1) (Supp. Feb. 1975).

2065. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(4) (Supp. Feb. 1975).

63-619 O - 76 - 86

termine individual qualifications for appointment or promotion in the federal service,"[2066] information obtained prior to the effective date of the Privacy Act under either an express or implied promise of confidentiality if release of the information would identify the source,[2067] information supplied by third parties under an express pledge of confidentiality after the effective date of the Act if disclosure would identify the source,[2068] and material relating to the subject's health, unless certain "special procedures" are established.[2069] The first three categories are reasonable: the last three, however, deserve special attention.

An agency may not conceal the existence of information in the fourth category—that obtained from third parties prior to the effective date of the Act—and must characterize it at least in some very general way.[2070] While the provision purports to recognize the privacy interests of those persons who supplied information under a promise of secrecy prior to the effective date of the Act, the provision fails to protect those interests completely. First, the provision does not require agencies to deny access to this information. Second, the provision only applies to investigatory material compiled for civil[2071] and criminal[2072] law enforcement purposes, investigatory material compiled for determining suitability for federal employment,[2073] evaluation material used to determine potential for promotion in the Armed Services,[2074] and material held by the CIA.[2075] While most third-party information collected by the federal government may fall into one of these three categories, the privacy interests of all persons who divulged information under an express or implied promise of confidentiality should be protected.

Under the fifth category, agencies are allowed to withhold the same types of third-party information obtained after the effective

2066. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(6) (Supp. Feb. 1975), allows the exemption of this material when "disclosure . . . would compromise the objectivity or fairness of the testing or examination process." This provision was designed to protect "actual competitive examinations and rating schedules." *Hearings on Access*, *supra* note 1969, at 290. It should not be interpreted, at it might be if read literally, to allow agencies to prevent access to the results of an individual's psychological tests. *Cf.* text at notes 2081-88 *infra*.

2067. Privacy Act § 3, 5 U.S.C.A. §§ 552a(k)(2), (k)(5), (k)(7) (Supp. Feb. 1975).

2068. Privacy Act § 3, 5 U.S.C.A. §§ 552a(k)(2), (k)(5), (k)(7) (Supp. Feb. 1975).

2069. Privacy Act § 3, 5 U.S.C.A. § 552a(f)(3) (Supp. Feb. 1975).

2070. 120 CONG. REC. H12,244 (daily ed. Dec. 18, 1974).

2071. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(2) (Supp. Feb. 1975).

2072. Privacy Act § 3, 5 U.S.C.A. § 552a(j)(2) (Supp. Feb. 1975). The exemption for criminal law enforcement agencies includes this and other information. *See* text at note 2169 *infra*.

2073. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(5) (Supp. Feb. 1975).

2074. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(7) (Supp. Feb. 1975).

2075. Privacy Act § 3, 5 U.S.C.A. § 552a(j)(1) (Supp. Feb. 1975). All files held by the CIA are exempted. *See* text at notes 2180-82 *infra*.

date of the Act, but only if the third parties were given an express promise of confidentiality. At the hearings on the Privacy Act, agencies emphasized the need to be able to promise confidentiality in order to get candid evaluations of employees[2076] and evidence or leads in law enforcement investigations.[2077] But, in light of the resulting infringement of the privacy interests of data subjects, there should be some requirement that pledges of confidentiality be granted only when necessary and only where there is a strong, clearly justified societal interest at stake.[2078] Criminal- and civil-law enforcement and national security seem to be two such interests. In the two other areas referred to by the Privacy Act, however, the societal interests at stake are arguably less important: representatives of some federal agencies have testified that they do not need the power to give pledges of confidentiality in order to carry out employment-related investigations,[2079] and it would seem that, absent national security implications, the military could also conduct promotion-related investigations without granting pledges of confidentiality. The reasonableness standard regulating methods of acquisition that was recommended above[2080] would subsume this whole question by limiting the instances in which information could be collected from confidential sources. This more flexible standard would both better protect the privacy interests of data subjects and aid agencies by allowing them to grant pledges of confidentiality in certain circumstances where they are not currently authorized to do so. It might, for example, allow agencies to withhold information revealing a confidential source where disclosure would endanger the physical safety of the informant.

The sixth category of information exempt from the notice and challenge provisions unnecessarily limits subject access to medical records by allowing an agency to establish "special" procedures for the disclosure to an individual of medical records, including psychological records, pertaining to him. The House report on the Act reveals that this provision was included because of the feeling that the transmission of medical information could have an adverse effect upon an

---

2076. The statement of the Department of Defense is typical: "It is almost axiomatic to observe that if persons who are interviewed know that the interview will be revealed to the subject of the file, that it would have a chilling effect on their willingness to give a forthright statement of what they know about the subject." *Hearings on Access*, *supra* note 1969, at 240.

2077. *See, e.g., id.* at 149 (statement of M. Lawton, Deputy Assistant Attorney General, Department of Justice).

2078. *Hearings on Access*, *supra* note 1969, at 162 (testimony of T. McFee, Deputy Assistant Secretary, HEW).

2079. *See, e.g., Joint Hearings*, *supra* note 1641, at 466 (testimony of the representative of the FTC).

2080. *See* text following note 2026 *supra*.

individual.[2081] In such a case the House report suggests that the agency could release the information to a doctor named by the requesting individual.[2082] The report would also allow an agency to adopt other rules to apprise a person of medical information about him. It is unclear what other procedures are envisioned, but the report seems to imply that an individual need not have complete access to his file, even after it is transmitted to his doctor. In certain respects, allowing patients access to their own records seems to be a better policy than selective disclosure. First, nonaccess of patients to their records may prevent the correction of innocent errors.[2083] Second, it is rather incongruous to allow doctors to decide what information a patient may have concerning himself, especially where there might be a question of malpractice.[2084] Third, involving patients in medical record-keeping helps establish good doctor-patient relations and contributes to the quality of health care.[2085] On the other side, it is urged that records should not be disclosed because they are in technical language that patients cannot understand. But this problem can more easily be remedied by ensuring that patients receive explanations of their records.[2086] It is also feared that disclosure to a patient that he has a terminal disease may cause him emotional and psychological harm.[2087] However, the policy that a doctor should decide whether a patient should be informed about his condition is paternalistic. At least one state has codified the patient's right of access to all medical records except those of mental hospitals.[2088] A similar approach in the Privacy Act would be more consistent with the Act's over-all policy of vesting control in the individual over the flow of information about him. In light of the layman's need for explication of much medical information, the agency should be allowed to insist on disclosure to a doctor designated by the subject, but the doctor should then be required to disclose the entire substance of the records to the subject.

A final concern with respect to the right of access is that the cost of the procedure to the subject not nullify the right. The Privacy Act authorizes agencies to charge fees only for the cost of making copies of the record,[2089] thereby sparing the subject the potentially large cost of search for and review of records.[2090] The Act also avoids

2081. H.R. REP. No. 93-1416, 93d Cong., 2d Sess. 16-17 (1974).

2082. *Id.*

2083. *Joint Hearings*, *supra* note 1641, at 2243-44 (report of B. Kaiser).

2084. *Id.* at 2244.

2085. *Id.* at 2242.

2086. *Id.*

2087. *See id.* at 2243.

2088. *See* MASS. ANN. LAWS ch. 111, § 70 (1975).

2089. Privacy Act § 3, 5 U.S.C.A. § 552a(f)(5) (Supp. Feb. 1975).

2090. The Director of the Bureau of Manpower Information Systems of the CSC

making the right of access illusory by not *requiring* the data subject to examine his file at the place it is kept. The Senate had advocated that individuals be allowed to receive copies of their files by mail upon written request and with proper identification,[2091] but as enacted the Act only requires each agency "to establish procedures for the disclosure to an individual" of his file.[2092] Although this provision would seem to allow an agency to use the mails, it unfortunately does not guarantee that data subjects will be able to resort to such a procedure.

Complementing the right of access is the other major provision of the Privacy Act, the right to challenge. Subsection (d)(2) fully incorporates the right of challenge with respect to all records to which the individual has a right of access. Together the rights of access and challenge enable the individual to ensure that the government maintains in its files only relevant and accurate information about him. Further, through challenge of inaccurate or irrelevant information the individual can exercise a deterrent effect on improper acquisition.

Under subsection (d)(2), each agency must, within ten days following receipt, acknowledge an individual's request to amend his record[2093] and promptly correct the record or inform the individual of its refusal to do so.[2094] The agency must also state its reasons for refusing to amend and inform the individual of the procedures established for the review of that refusal.[2095] If the individual seeks such a review, it must be conducted within thirty days. If after review the agency still refuses to amend the record, it is required to notify the individual of his right to file with the agency a concise statement setting forth his disagreement with the agency,[2096] and it must inform him of his right to seek judicial review in the federal district courts.[2097] Subsection (d)(4) requires the agency to note

has stated that the cost for a search of computerized records is $35 per hour. *See Hearings on Access, supra* note 1969, at 306.

2091. *See* S. REP. No. 93-1183, *supra* note 1977, at 61.

2092. Privacy Act § 3, 5 U.S.C.A. § 552a(f)(3) (Supp. Feb. 1975).

2093. Privacy Act § 3, 5 U.S.C.A. § 552a(d)(2)(A) (Supp. Feb. 1975).

2094. Privacy Act § 3, 5 U.S.C.A. § 552a(d)(2)(B) (Supp. Feb. 1975).

2095. Privacy Act § 3, 5 U.S.C.A. § 552a(d)(2)(B)(ii) (Supp. Feb. 1975).

2096. Privacy Act § 3, 5 U.S.C.A. § 552a(d)(3) (Supp. Feb. 1975). In hearings on the Privacy Act, the Director of the Bureau of Manpower Information Systems of the CSC stated, "A requirement to accept even a reasonable amount of supplementary material of the individual's choosing for inclusion in the automated systems would result in sharply increased operating costs, and with respect to some of these systems we are planning, could make the systems completely impractical." *Hearings on Access, supra* note 1969, at 291. The Act apparently solves this problem by allowing an agency to note the existence of the statement in the computerized file but file the statement itself separately.

2097. Privacy Act § 3, 5 U.S.C.A. § 552a(d)(3) (Supp. Feb. 1975). For a discussion of the judicial review provisions of the Act see text at notes 2129-38 *infra*.

clearly the disputed portions of the record and to provide copies of the individual's statement of disagreement to any person or agency to whom the record is subsequently disclosed. Subsection (c)(4) requires the agency to notify all persons or agencies to whom the disputed record has already been disseminated of the dispute and of the individual's statement of correction. While the statutory scheme is quite comprehensive, it has a few minor deficiencies.

First, until an individual has filed a statement of disagreement, an agency may disseminate challenged information without noting the challenge. Thus, for at least a month, an agency can circulate incorrect information. As there would be little additional administrative burden in noting the initial amendment request in the individual's record, the disseminating agency should be required to do so before releasing the file to other agencies. It does not appear as necessary to require immediate notification of the dispute to prior recipients, in view of the substantial administrative burden entailed in notifying them, and in light of subsection (c)(4)'s requirement that they be notified after the individual has filed a statement of disagreement.

Second, although subsection (c)(4) requires an agency to notify prior agency recipients when it amends a file, it does not require the recipent agencies to amend their files also, as the Senate apparently intended.[2098] The requirement in subsection (e)(1) that each agency maintain only relevant information may be interpreted to require the recipient agency at least to investigate the accuracy of the information, but this requirement applies only to recipient agencies that are covered by the Act. Rather than burdening the individual with the responsibility of asking each recipient agency whether his record has been amended, it would seem more sensible to require recipient agencies that decide not to amend so to notify the individual.

The Privacy Act also addresses possible threats to privacy posed by agency alteration of information systems. Subsection (o) of the Act requires each agency to provide adequate notice to Congress of any proposal to establish or alter any system of records in order to permit Congress to make an evaluation of the proposal's potential effect on the right of privacy. This provision, in conjunction with the subsection (e)(4) requirement that a description of each existing information system be published in the *Federal Register*,[2099] should prevent the maintenance of any secret information systems. Subsection (o) was also intended to prevent the creation of data banks without statutory authorization and without proper regard for individual privacy, the confidentiality of data, and the security of the

2098. *See* S. Rep. No. 93-1183, *supra* note 1977, at 62.

2099. *See* note 2052 *supra* and accompanying text.

system,[2100] and to prevent the development of a de facto national data bank.[2101] This final fear is justified, for while an express proposal for a National Data Bank Center was defeated in the mid-1960's,[2102] the possibility that agencies will consolidate information systems on their own has remained.[2103] Regardless of the merits of the centralization of information systems,[2104] it should not occur without congressional oversight. Subsection (o) accords Congress the opportunity to give that oversight. Subsection (o)'s main deficiency is that it only requires an agency to report proposals to Congress so that it can evaluate the idea. As it will eventually be necessary to obtain the agency's own views on the proposal, Congress should have required, as the Senate bill proposed,[2105] that each agency evaluate

---

2100. S. REP. No. 93–1183, *supra* note 1977, at 64-65.

2101. *Id.* at 64.

2102. Several such recommendations were made. *See* SUMMARY AND CONCLUSIONS, *supra* note 1515, at 8-9. For a complete discussion of the proposal see Note, 82 HARV. L. REV. 400, *supra* note 1909.

2103. *See Hearings on the Census*, *supra* note 1509, at 181 (testimony of A. Miller, Professor, University of Michigan Law School). *See also Joint Hearings*, *supra* note 1641, at 2252-55.

2104. Advocates of the national data-bank center thought it would: (1) make more data available for researchers; (2) reduce the unit cost of data; (3) enable larger and more effective samples to the taken; (4) facilitate the canvassing of a wider range of variables; (5) reduce duplication in government data collection activities; (6) promote greater standardization of techniques among the agencies; (7) make research efforts easier to verify; and (8) provide a data processing pool for all the information-handling agencies. A. MILLER, *supra* note 1503, at 56-57. *See* Sawyer & Schechter, *Computers, Privacy and the National Data Center: The Responsibility of Social Scientists*, 23 THE AM. PSYCHOLOGIST 810, 813 (1968). However, the merits of the proposal were never really given fair consideration. Instead, the proposal became a focal point for the fears of a loss of privacy. *See, e.g.*, A. MILLER, *supra*, at 57; Hirsch, *Data Banks: The Punchcard Snoopers*, 205 NATION 369 (1967); Miller, *The National Data Center and Personal Privacy*, ATLANTIC, Nov. 1967, at 53; U.S. NEWS & WORLD REP., May 16, 1966, at 56. Numerous congressional hearings were held, outlining the dangers of consolidation. *See* SUBCOMM. ON ECONOMIC STATISTICS OF THE JOINT ECONOMIC COMM., 90TH CONG., 1ST SESS., REPORT ON THE COORDINATION AND INTEGRATION OF GOVERNMENT STATISTICAL PROGRAMS (Joint Comm. Print 1967); *Hearings on the Coordination and Integration of Government Statistical Programs Before the Subcomm. on Economic Statistics of the Joint Economic Comm.*, 90th Cong., 1st Sess. (1967); *Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess. (1967); *Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966). It was feared that even statistical data could be used to injure individuals, that improved capacity for handling data would result in demands for more personal information, that reliance upon computers to make decisions affecting personal affairs would be increased, that individualized output would eventually be permitted, and that the center by its very existence would increase conformity by compelling people to "act for the record." Note, *supra* note 1909, at 411-12. The criticism of the bill was so overwhelming that the National Data Center concept is still not a realistic legislative proposal. SUMMARY AND CONCLUSIONS, *supra* note 1515, at 10.

2105. *See* S. 3418, § 201(f)(1), 93d Cong., 2d Sess. (1974).

the effect of its proposal in a privacy impact statement and submit that statement along with the proposal.[2106]

4. *Dissemination*

The great number of transfers of personal information pose a grave danger to privacy interests. The Privacy Act deals with this problem by allowing dissemination for "routine" uses, by prohibiting dissemination for "nonroutine" uses without the prior written consent of the subject,[2107] and by requiring that the individual be notified at the time of collection of the routine uses that may be made of the information.[2108] Subsection (a)(7) defines "routine use" as "use . . . for a purpose which is compatible with the purpose for which the information was collected." A further limitation on dissemination is that transferee agencies subject to the Act must meet the subsection (e)(1) requirement that agencies maintain only relevant and necessary information.

The present provisions represent a compromise between the proposal that no records be disclosed outside the collecting agency without the prior consent of the subject,[2109] and the proposal that agencies be free to disclose information to anyone as long as the subject is notified.[2110] The former proposal ignored the costly duplication of effort that would be required if individuals chose to prevent all transfers,[2111] while the latter gave insufficient weight to the right of an individual to control the flow of information about him. As discussed below,[2112] the Act made no substantive change in the law regarding the disclosure of personal information.[2113]

The scheme adopted by the Privacy Act is subject to attack on the ground that it gives insufficient control to the subject at the time of data acquisition. For example, although each agency must inform the information supplier of the routine uses that may be made of the information, the Act does not recognize a right to withhold information on the basis of the agency's determination of routine uses.

2106. *See* S. REP. No. 93-1183, *supra* note 1977, at 64-65.

2107. Privacy Act § 3, 5 U.S.C.A. § 552a(b) (Supp. Feb. 1975).

2108. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(3) (Supp. Feb. 1975). Subsection (e)(4)(D)'s requirement that each agency publish "each routine use of the records contained in the system, including the categories of users and the purpose of such use" provides additional notice.

2109. *See* H.R. 9527, 92d Cong., 2d Sess. (1972).

2110. *See* H.R. 12206, 93d Cong., 2d Sess. (1974).

2111. For example, every three months the Social Security Administration transfers the earning records of one million persons to state agencies that administer unemployment programs. If consent for the transfer were required and refused, the states would have to acquire this information on their own. Even a notice requirement would be unreasonably costly, resulting in four million notices a year. *See Hearings on Access*, *supra* note 1969, at 182.

2112. *See* text at note 2198 *infra*.

2113. *See* 11 WEEKLY COMP. OF PRES. DOCS. 8 (Jan. 1, 1975).

Instead, the Act envisions that Congress will exercise "a vigorous oversight check on agencies to make certain as much as possible that no 'nonroutine' transfers of records . . . are either hidden or blanketed in under the 'routine' category to nullify the basic protections of the law to individuals."[2114] Each agency thus can, absent congressional action, continue to decide the uses for which it can disseminate information it collects;[2115] the SEC's Name and Relationship System, for example, can continue routinely to distribute derogatory information to other agencies,[2116] and the Civil Service Commission can continue routinely to transmit information on a subject's character, general reputation, personal characteristics, and mode of living to various branches of the government.[2117] To be sure, once unnecessary or irrelevant information is transferred to an agency for a routine use, the individual presumably can challenge the retention of that information under subsection (e)(1). Moreover, individuals can trace distributions of their records because of the (c)(3) requirement that agencies make available to the subject accountings of file transfers. These two subsections provide only limited control over the dissemination of information, however, because they apply only after dissemination has occurred and they depend on the subject initiating an inquiry as to whether there have been improper disseminations. To ensure that individuals retain control over the dissemination of surrendered information, the Privacy Act should have required that the individual be able to challenge collection by the collecting agency on the ground that the information sought is irrelevant to or unneeded by an agency that has been labeled a routine recipient.

Subsection (b) allows dissemination of records for nonroutine uses without the prior consent of the individual in a variety of situations where the need for the information is great or the damage to privacy interests is slight.[2118] For example, subsection (b)(4) allows

2114. H.R. REP. No. 93-1416, *supra* note 2081, at 12.

2115. Moreover, Privacy Act, § 3, 5 U.S.C.A. § 552a(e)(11) (Supp. Feb. 1975), allows an agency to publish in the *Federal Register* notice of any new use and provide an opportunity for interested persons to submit arguments. The provision would apparently allow an agency to adopt new "routine uses" for which disclosure could be made without the data subject's consent.

2116. *See* FEDERAL DATA BANKS, *supra* note 1515, at XLIV.

2117. *See id.*

2118. There are ten situations where information may be disseminated for a nonroutine use without the prior consent of the individual. Five of these are discussed in the text at notes 2119-23 *infra*. The other five situations seem inoffensive. Subsection (b)(1) allows disclosure of the information to those officers and employees of the agency maintaining the record who need the record to perform their duties. Subsection (b)(6) allows disclosure to the National Archives. This exemption allows an agency to gather information of historical importance. For its legislative origin see *Hearings on Access, supra* note 1969, at 274-76. Subsection (b)(8) allows disclosure "to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual." Subsection (b)(9), allowing dissemination to Congress, and

disclosure of records to the Bureau of the Census for purposes of planning because of the strict confidentiality of Census records.[2119] Subsection (b)(5) permits disclosure of records in a nonidentifiable form to a recipient for use in statistical research because of the reduced privacy dangers in the transfer of nonidentifiable information and because of the desire to facilitate research.[2120] Subsection (b)(7) exempts from the consent requirement information sought by an agency for a law enforcement activity, but prevents law enforcement agencies from going on "fishing expeditions" by requiring the head of the requesting agency to specify in writing the particular portion of the record desired and the law enforcement activity for which the record is sought.

Only two of the exemptions are questionable. Subsection (b)(11) allows disclosure without consent "pursuant to the order of a court of competent jurisdiction." The Senate recommended that an agency be required to serve advance notice on the subject before it disseminates his file pursuant to compulsory legal process.[2121] Such a provision is more attractive than the provision adopted because it affords greater protection to the subject's privacy interests by permitting him to take appropriate legal steps to suppress a subpoena[2122] without unduly burdening the requester, who would already be in court. The difficulties with subsection (b)(2), which permits disclosures required under the FOIA, are dealt with in the discussion on the interaction of the Privacy Act and the FOIA.[2123]

Subsection (n) of the Privacy Act deals with a narrow dissemination problem that had attracted earlier congressional attention,[2124] by forbidding the sale or rental by an agency of an individual's name and address unless such action is specifically authorized by law. The provision was a response to the practice of various government agencies of selling mailing lists of persons with certain characteristics, such as gun collectors, amateur radio operators, and licensed pilots, to commercial and political organizations.[2125] The sale of such lists infringes upon privacy interests not because the individual receives mail, which can easily be thrown away, but because information

---

subsection (b)(10), allowing dissemination to the Comptroller General, facilitate oversight of the administration of the Act.

2119. Laws relating to the Bureau of the Census limit access to census records to Bureau employees and prohibit their removal from the premises. H.R. REP. No. 93–1416, *supra* note 2081, at 12-13. *See* text at notes 1934-35 *supra*.

2120. *See also Hearings on Access*, *supra* note 1969, at 159, 180-81 (remarks of the representative of HEW).

2121. *See* S. REP. No. 93–1183, *supra* note 1977, at 66.

2122. *See id.*

2123. *See* text at notes 2196-214 *infra*.

2124. *See generally Hearings on Mailing Lists*, *supra* note 1499.

2125. *See id.* at 28-29, 70, 136.

about the individual has been disclosed without his knowledge. Although salutary in purpose, subsection (n) may be of limited force because it states explicitly that it shall not be construed to require the withholding of names and addresses otherwise permitted to be made public, and presumably, therefore, permits disclosure under the FOIA.[2126] Provisions of the FOIA mandating disclosure of information to the public do not apply where disclosure "would constitute a clearly unwarranted invasion of personal privacy."[2127] This privacy exemption to the FOIA, however, does not as interpreted adequately protect privacy interests.[2128] In the area of mailing lists, its disabilities are perpetuated in the Privacy Act because of subsection (n).

5. *Remedies and Sanctions*

The privacy rights created by the Privacy Act would be meaningless if they were not accompanied by effective remedies or sanctions. The Act establishes civil and criminal liability for some violations, but it seems doubtful that such provisions are sufficient to protect all the rights created by the Act.

Subsection (g)(1) of the Privacy Act provides that an individual may bring a civil action against an agency in the federal district courts whenever the agency refuses to amend the individual's record[2129] or refuses access to a record.[2130] Thus an individual always has standing to contest an agency's failure to accord him the rights of access and challenge. An individual's standing to contest an agency's failure to maintain his records with accuracy, relevance, timeliness, and completeness, set forth in subsection (g)(1)(C), extends only to situations in which a determination is made that is adverse to the individual. Subsection (g)(1)(C) apparently refers to violations of subsection (e)(5) only; but might also include violations of (e)(1). Because the next subsection states only that it applies to violations of "any other provision,"[2131] it is left unclear whether an individual alleging a violation of (e)(1) must await an adverse determination as required by (g)(1)(C).

With respect to violations of all other primary rights conferred by the Act, subsection (g)(1)(D) grants standing to an individual whenever an agency "fails to comply with any other provision of this section, . . . in such a way as to have an adverse effect on the individual." While the provision presumably does not require an

---

2126. 120 CONG. REC. H12,244 (daily ed. Dec. 18, 1974).

2127. 5 U.S.C. § 552(b)(6) (1970).

2128. *See* text at notes 700-44 *supra*.

2129. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(1)(A) (Supp. Feb. 1975).

2130. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(1)(B) (Supp. Feb. 1975).

2131. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(1)(D) (Supp. Feb. 1975).

adverse administrative determination, the ambiguity of the term "adverse effect" leaves unclear what an individual must show to obtain standing. If the adverse effect requirement is only intended to restrict standing to data subjects whose Privacy Act rights are violated (through, for example, improper dissemination or improper collection of information), the subsection would impose only minimal standing requirements. If, however, the adverse effect requirement is intended to restrict standing to individuals who can prove prima facie that the agency violation resulted in monetary harm,[2132] the Act would fail to recognize that there can be serious violations of privacy that do not result in such harm.[2133]

The argument that the adverse effect requirement allows suit by anyone who is the subject of information acquired or disseminated in violation of the Privacy Act draws support from the Senate report on an analogous provision contained in the Senate bill. Although the phrase "adverse effect" comes from the House bill,[2134] the Senate version granted standing to any "aggrieved person,"[2135] a similar formulation. The Senate report explained that the phrase was

> designed to encourage the widest possible citizen enforcement through the judicial process. This is necessary, as mentioned, since the Act does not give any administrative body authority to ensure compliance with the Act. The Committee intends the use of the term "aggrieved person" to afford the widest possible standing consistent with the constitutional requirement of "case or controversy" in Article III, Sec. 2 of the Constitution. In this respect, the provision is designed, among other things, to supply certain deficiencies in standing and ripeness which the courts found in *Environmental Protection Agency* v. *Mink*, 410 U.S. 73 (1973), *Laird* v. *Tatum*, 408 U.S. 1 (1972), and [*California Bankers Association* v. *Shultz*, 416 U.S. 21 (1974)].[2136]

The failure of the conference staff's report to comment on any compromise in this regard arguably suggests that the House conferees understood their language to have the same effect. If Congress had intended to require a showing of actual damage in order to obtain standing, it could have used the words "actual damages," as it did in subsection (g)(4)(A), instead of "adverse effect."

There are countervailing indications, however, that the "adverse effect" requirement of subsection (g)(1)(D) was intended to require

---

...aird v. Tatum, 408 U.S. 1, 13-14 (1972) (rejecting a challenge to use of ... for domestic surveillance and holding that "[a]llegations of a subjective ... an adequate substitute for a claim of specific present objective harm or ... of specific future harm . . .").

2133. *See* text at notes 1536-49 *supra*.

2134. *See* H.R. 16373, § (g)(1)(C), 93d Cong., 2d Sess. (1974).

2135. S. 3418, §§ 303(b), (c), 93d Cong., 2d Sess. (1974).

2136. S. REP. No. 93-1183, *supra* note 1977, at 88.

a showing of actual harm. This conclusion is supported by the structure of subsection (g)(1). Subsections (g)(1)(A) and (g)(1)(B), providing standing when an agency violates subsections (d)(3) or (d)(1) of the Act, clearly do not require a showing of actual harm. If subsection (g)(1)(D) were meant to give standing to any individual who is affected by any other violations of the Act, there would have been no need to mention specifically violations of (d)(3) and (d)(1) in subsections (g)(1)(A) and (g)(1)(B). Moreover, the wording of subsection (g)(1)(D) comes directly from the language of the House bill,[2137] which is generally more conservative in its protections of the right of privacy.[2138]

Given these conflicting indications of congressional intent, courts should interpret "adverse effect" broadly, and should not require a showing of actual harm. This interpretation of "adverse effect" is necessary if the Act is to fulfill its stated purpose to "permit an individual to determine what records pertaining to him are . . . disseminated . . . ."[2139] If an individual can only challenge the dissemination of information that causes him monetary harm he is obviously powerless to prevent much improper dissemination.

The Act grants either damages or injunctive relief, depending upon the nature of the agency violation, to individuals with standing to sue. When an agency improperly refuses to amend an individual's record or improperly refuses an individual access to his records, the Act authorizes courts to order the agency to correct the record or to produce the record.[2140] In these situations, the Act makes injunctive relief the exclusive remedy, with no provision for redress of actual damages suffered from wrongful agency refusal to amend. For all other violations of the Act the sole remedy appears to be monetary damages.[2141] Damages are not available, however, unless "the agency

---

2137. *See* H.R. 16373, § (g)(1)(C), 93d Cong., 2d Sess. (1974).

2138. See the various Senate proposals mentioned at notes 2091, 2121, & 2136 *supra*, and at notes 2145, 2147, 2151, & 2182 *infra*.

2139. Privacy Act § 2(b)(1), 5 U.S.C.A. § 552a (note) (Supp. Feb. 1975).

2140. Privacy Act § 3, 5 U.S.C.A. §§ 552a(g)(2), (g)(3) (Supp. Feb. 1975). Where the violation alleged is refusal to amend, subsection (g)(2)(A) empowers the court to determine the matter de novo. Where the violation alleged is denial of access to a file, subsection (g)(3)(A) empowers the court to determine the matter de novo and to examine in camera the contents of any records claimed to be exempted by subsection (k), discussed in the text at notes 2183-94 *infra*. In an action under either (g)(2) or (g)(3), the court may assess against the United States reasonable attorney fees and other reasonable litigation costs, if the complainant has substantially prevailed. Privacy Act § 3, 5 U.S.C.A. §§ 552a(g)(2)(B), (g)(3)(B) (Supp. Feb. 1975).

2141. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(4) (Supp. Feb. 1975) provides:

> In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—
>
> (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

acted in a manner which was intentional or willful. . . ."[2142] This standard for recovery of damages is a compromise[2143] between the House proposal of the traditional "arbitrary and capricious" standard for review of agency action[2144] and the Senate proposal of strict liability for any agency violation of the Act.[2145] The legislative history indicates that "[o]n a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed as only somewhat greater than gross negligence."[2146] This comment suggests that liability should not attach unless the agency's action was so lacking in reason as to approach recklessness. This requirement obviously imposes a heavy burden on a party seeking compensation. As the Act does not explicitly provide for injunctive relief for these violations, a plaintiff who fails to meet this requirement may be without a remedy. For example, a court might find that an agency is improperly disseminating files for nonroutine uses without the subjects' consent, and yet be powerless not only to prevent the dissemination but also to grant compensation to the subjects. This interpretation is one courts might well try to avoid, but the Act could have avoided this difficulty either by authorizing injunctive relief with regard to all violations of the Act where appropriate,[2147] or by setting a lower standard for agency liability, or both.

Under the Act, damages are to be recovered from the federal government.[2148] If the offending agency were required to pay, such payments would be reflected in the agency's operating budget and would perhaps provide a more direct deterrent to violations. The $1000 floor on recovery provided in the Act[2149] presumably represents a compromise between the House proposal, which only allowed recovery of actual damages,[2150] and the Senate proposal, which allowed recovery of punitive damages where appropriate.[2151] A provision for punitive damages would seem desirable in order to deter repeated violations of the Act, although in the absence of direct

---

(B) the costs of the action together with reasonable attorney fees as determined by the court.

2142. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(4) (Supp. Feb. 1975).

2143. 120 CONG. REC. H12,245 (daily ed. Dec. 18, 1975).

2144. H.R. 16373, § (g)(3), 93d Cong., 2d Sess. (1974).

2145. S. 3418, § 303(c), 93d Cong., 2d Sess. (1974).

2146. 120 CONG. REC. H12,245 (daily ed. Dec. 18, 1974).

2147. S. 3418, § 303(b), 93 Cong., 2d Sess. (1974), would have so provided.

2148. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(4) (Supp. Feb. 1975), set out in note 2141 *supra*.

2149. Privacy Act § 3, 5 U.S.C.A. § 552a(g)(4)(A) (Supp. Feb. 1975).

2150. *See* H.R. 16373, § (g)(3)(A), 93d Cong., 2d Sess. (1974).

2151. *See* S. 3418, § 303(c)(2), 93d Cong., 2d Sess. (1974).

recovery from the offending agency, the effectiveness of such deterrence is certainly questionable.

In sum, the Privacy Act allows a data subject to enforce his rights of access and challenge through injunctive relief, and provides him with an opportunity to collect damages for the "intentional or willful" retention of inaccurate or irrelevant information once an agency has made a determination adverse to his interests. Thus, the Act provides relatively full protections against violations of privacy that occur in the retention stage. With respect to the acquisition and dissemination stages, however, the remedies provided by the Act are clearly unsatisfactory. Only damages are available, and to obtain them the plaintiff must show that the agency acted intentionally and willfully, and may have to show actual harm. The weakness of the remedy provisions prevents the accomplishment of the Act's purpose to "permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated . . . ."[2152] To accomplish this purpose, the Act should have given standing to anyone who is the subject of information involved in a violation of the Privacy Act and should have provided for actual damages, punitive damages, and injunctive relief, wherever appropriate, as the Senate bill had proposed.[2153]

For violations of provisions that are "key to any effective protection for privacy and confidentiality,"[2154] the Act provides criminal fines of up to $5000. Because "[t]he entire Act would be frustrated if secret data banks could be created and operated with impunity,"[2155] subsection (*i*)(2) imposes a fine on "[a]ny officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of [publishing in the *Federal Register*] . . . ." In response to the equally fundamental need to guard against willful disregard of the limitations on dissemination,[2156] subsection (*i*)(1) imposes fines on any officer or employee of an agency "who knowing that disclosure of the specific material is . . . prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it . . . ." Finally, subsection (*i*)(3) makes "[a]ny person who knowing and willfully requests or obtains any record concerning an individual from an agency under false pretenses . . ." subject to a fine. None of the civil remedies in the Act would reach individuals guilty of such violations. At least one other critical provision of the Act probably should have been

2152. Privacy Act § 2(b)(1), 5 U.S.C.A. § 552a (note) (Supp. Feb. 1975).

2153. S. 3418, §§ 303(b), (c), 93d Cong., 2d Sess. (1974).

2154. S. Rep. No. 93-1183, *supra* note 1977, at 81.

2155. *Id.*

2156. *Id.*

reinforced by criminal penalties. Because all of the rights granted by the Privacy Act depend on an individual's ability to find out if an agency maintains a file on him, the Act should have imposed criminal liability on any officer or employee of an agency who, in response to an individual's inquiry about the existence of a file, knowingly responds falsely.

As an aid in enforcing and administering the Privacy Act, the establishment of a federal privacy board was recommended.[2157] As enacted, however, the Privacy Act envisions that disputes arising under it will be settled in the federal courts, and delegates to the agencies themselves the task of promulgating regulations governing the administration of the Act.[2158] A federal privacy board has definite advantages, for it could reduce the case-load burden of the district courts, promote uniformity by promulgating regulations implementing the Act for all agencies,[2159] and reduce the possibility of infractions of the Privacy Act by conducting on-site audits of agency information systems and files.[2160] The board also could be charged with the administration of the FOIA, thereby providing oversight of the interaction between the Privacy Act and the FOIA. Apparently the privacy board proposal failed because Congress was reluctant to establish yet another federal bureaucracy,[2161] and because the administrative costs would have been great. Instead, the Privacy Act establishes a Privacy Protection Study Commission, empowered merely to study agency information practices and to recommend changes in the Privacy Act.[2162]

6. *Exemptions*

The two exemptions to the several provisions of the Privacy Act are, in general, necessary and reasonably circumscribed. Subsection (j)(2) allows criminal law enforcement agencies to exempt certain types of records that they maintain from the provisions granting the rights of subject notice, access, and challenge,[2163] restricting the

2157. Representative Koch, who introduced the first privacy bill, favored creation of a Federal Privacy Board. *See* 120 CONG. REC. H12,248 (daily ed. Dec. 18, 1974). S. 3418, §§ 101-07, 93d Cong., 2d Sess. (1974), incorporated the idea, but H.R. 16373, 93d Cong., 2d Sess. (1974), did not establish any type of board to oversee administration of the Act.

2158. Privacy Act § 3, 5 U.S.C.A. § 552a(f) (Supp. Feb. 1975), requires each agency to establish procedures governing notice, access, and challenge.

2159. S. 3418, § 103(a)(3), 93d Cong., 2d Sess. (1974), gave the board authority to "develop model guidelines" and "assist Federal agencies in preparing regulations."

2160. This power was explicitly given to the board in the original version of S. 3418, introduced on May 1, 1974. The version reported from committee and passed by the Senate, however, gave the board the power to conduct "inspections." S. 3418, § 103(a)(3), 93d Cong., 2d Sess. (1974).

2161. *See, e.g., Hearings on Access, supra* note 1969, at 195.

2162. Privacy Act § 5, 5 U.S.C.A. § 552a (note) (Supp. Feb. 1975).

2163. Privacy Act § 3, 5 U.S.C.A. § 552a(d) (Supp. Feb. 1975), discussed in the text

acquisition of data[2164] and the method of acquisition,[2165] requiring accuracy of retained information,[2166] imposing civil liability,[2167] and requiring notice to Congress of any alteration of its system of records.[2168] The types of records that may be exempted consist of:

> (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.[2169]

This list seems to encompass all records held for criminal law enforcement purposes. The exemption thus reflects a decision to leave the regulation of these records to separate legislation,[2170] and reveals a general fear of hampering criminal investigations[2171] by disclosing investigatory techniques[2172] or by discouraging the cooperation of informants.[2173]

In general, this law enforcement records exemption is reasonable. The exemption from restrictions on the type of information that may be acquired seems necessary because of the difficulty in deter-

---

at notes 2055-98 *supra*. These agencies can also exempt themselves from subsections (e)(4)(G)-(I), which require publication of the procedures for notice and access, and from subsection (f), which requires each agency to establish procedures for subject notice, access, and challenge.

2164. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(1) (Supp. Feb. 1975), discussed in the text at notes 1987-2003 *supra*.

2165. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(2) (Supp. Feb. 1975), discussed in the text at notes 2020-26 *supra*.

2166. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(5) (Supp. Feb. 1975).

2167. Privacy Act § 3, 5 U.S.C.A. § 552a(g) (Supp. Feb. 1975), discussed in the text at notes 2129-53 *supra*.

2168. Privacy Act § 3, 5 U.S.C.A. § 552a(*o*) (Supp. Feb. 1975), discussed in the text at notes 2099-106 *supra*.

It is possible that the exemption from subsection (*o*) is an oversight. The exemptions for agencies appear in subsections (j) and (k). No reference is made in these subsections to any other provision following subsection (k), most of which are relatively minor. However, the failure to deal with these later provisions means that the CIA and criminal law enforcement agencies can exempt themselves from the restrictions on the sale of mailing lists, *see* text at notes 2124-28 *supra*, and the development of new information systems. *See* text at note 2179 *infra*.

2169. Privacy Act § 3, 5 U.S.C.A. § 552a(j)(2) (Supp. Feb. 1975).

2170. *See* H.R. REP. No. 93-1416, *supra* note 2081, at 18.

2171. *See Hearings on Records, supra* note 1517, at 88-90 (Department of Justice), 110 (Department of Defense).

2172. *Id.* at 89-90 (Department of Justice).

2173. *Id.*

63-619 O - 76 - 87

mining what will be relevant to a criminal investigation; the exemption from the restrictions on method of acquisition is necessary because collection directly from the individual is generally inconsistent with the nature of criminal investigations. If the broader "reasonableness" standard for acquisition methods proposed above[2174] is adopted, however, a separate exemption would not be necessary because the standard takes into account the legitimacy and weight of agency needs and purposes. The exemption from the requirement that information used in a determination about an individual be accurate seems solidly grounded because the requirement's purpose, "to assure fairness to the individual in the determination,"[2175] is adequately guaranteed by the rules of procedure in a criminal trial.

There are, however, several respects in which the law enforcement records exemption is unduly broad. The first area in which narrowing is feasible is the area of subject access. The Senate bill had exempted from the right of subject access only information in the hands of criminal enforcement agencies that, if disclosed to the subject, would impede current law enforcement proceedings.[2176] Recent amendments to the FOIA have replaced an exemption similar to the Privacy Act's subsection (j)(2)(B) with an exemption allowing nondisclosure only where disclosure would interfere with law enforcement proceedings, deprive a person of his right to a fair trial, constitute an unwarranted invasion of privacy, disclose the identity of confidential sources who are protected by the provisions of the Act, disclose investigate techniques or procedures, or threaten the life or physical safety of law enforcement personnel.[2177] It is curious that Congress found it necessary to enact a broad provision in the Privacy Act when it had been satisfied with a more tailored exemption to the FOIA. Also, there seems to be no reason to exempt criminal law enforcement agencies from civil liability for violations of the few provisions that do apply to them. While criminal penalties remain applicable to violations of many of those provisions, they do not compensate the aggrieved individual. Improper disclosure of investigatory material to employers, for example, could seriously harm innocent individuals.[2178] Finally, the exemption to the requirement that Congress be notified of any alteration in the agency's system of records seems inexplicable, especially in light of the recent

2174. *See* text following note 2026 *supra*.

2175. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(5) (Supp. Feb. 1975).

2176. S. 3418, § 203(b), 93d Cong., 2d Sess. (1974).

2177. 5 U.S.C.A. § 552(b)(7) (Supp. Feb. 1975). *See* text at notes 745-828 *supra*.

2178. The ACLU presented a number of examples of individuals who lost jobs or were subjected to police harassment because of the dissemination of arrest records or intelligence information. *Hearings on Criminal Justice Data Banks*, *supra* note 1550, at 252-59.

congressional concern over proposed consolidation of criminal information systems.[2179]

Subsection (j) also allows the CIA to exempt any of its records from the same provisions. The purpose of the exemption appears to be the protection of national security interests.[2180] Yet the Act already contains a narrower exemption for classified documents,[2181] and there seems to be no reason to exempt all CIA records, since a blanket exemption would undoubtedly protect many records without any national security significance.[2182]

A narrower exemption in subsection (k) authorizes any agency to exempt certain specific records from the provisions dealing with subject notice, access, and challenge[2183] and from those concerning acquisition of data.[2184] The subsection covers classified documents,[2185] investigatory material compiled for civil law enforcement purposes,[2186] Secret Service files,[2187] testing or examination material con-

---

2179. *See id. passim.* The FBI has consolidated files on over 20 million individuals and computerized records on over 450,000 persons. *Id.* at 17. There are no formal regulations concerning distribution of these records. *Id.* at 18-19. The FBI currently has limited programs for sharing criminal information, *id.* at 10, and because of the growing concern over organized crime, with its interstate ramifications, there has been more and more pressure to consolidate investigative records. *Id.* at 18.

2180. *See* H.R. REP. No. 93–1416, *supra* note 2081, at 18.

2181. *See* text at note 2185 *infra.*

2182. The Senate had proposed a narrower exemption because "[m]any personnel files and other systems may not be subject to security classification or may not cause damage to the national defense or foreign policy simply by permitting the subjects of such files to inspect them and seek changes in their contents under this Act." S. REP. No. 93–1183, *supra* note 1977, at 74.

2183. Privacy Act § 3, 5 U.S.C.A. §§ 552a(d), (c)(3), (c)(4)(G), (H), (I), (f) (Supp. Feb. 1975).

2184. Privacy Act § 3, 5 U.S.C.A. § 552a(e)(1) (Supp. Feb. 1975).

2185. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(1) (Supp. Feb. 1975), exempts records "subject to the provisions of section 552(b)(1) of this title." *See* text at notes 506-35 *supra.*

2186. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(2) (Supp. Feb. 1975) exempts:

> (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

Representative Koch had argued that no exemption was needed for civil law enforcement agencies. 120 CONG. REC. H12,248 (daily ed. Dec. 18, 1974). Two factors may differentiate criminal law enforcement agencies. First, the prevention of crime is usually thought to be a more fundamental societal goal. Second, suspected criminals are protected from deprivations of benefits by stricter constitutional guarantees. Yet, a representative of the FTC testified that failure to protect its files from access would "wreak havoc on their ability to enforce their . . . statutes." *Hearings on Access, supra* note 1969, at 266-67.

cerning federal employment,[2188] and information that would reveal the identity of an informant where such information was obtained in order to determine suitability or eligibility for federal employment, military service, federal contracts, for access to classified information,[2189] or for promotion in the armed services.[2190]

Subsection (k) also exempts records "required by statute to be maintained and used solely as statistical records."[2191] Subsection (a)(6) defines a "statistical record" as "a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13." This last clause accommodates Census Bureau records.[2192] The exemption from the subject notice, access, and challenge provisions is reasonable because access and challenge would frustrate the timely production and dissemination of data. The exemption from restrictions on data acquisition, however, is unwise, for the result is to leave unregulated the types of irrelevant questions for which the census and other federal questionnaires have been criticized[2193] and to overlook the dangers to privacy from unrestrained acquisition of data.[2194]

To prevent the exemptions from swallowing the Privacy Act in practice, subsection (p) provides that the President shall submit to Congress an annual report "listing for each Federal agency the number of records . . . exempted from the application of [the Privacy Act] under the provisions of subsections (j) and (k). . . ." Congress recently added a similar provision to the FOIA to facilitate congressional oversight of the exemptions to that Act.[2195]

7. *Interaction Between the FOIA and the Privacy Act*

It is obvious that the public's right to know about government conduct, guaranteed by the FOIA, will sometimes collide with the equally important right guaranteed by the Privacy Act to control the flow of personal information. The balancing of interests required to resolve this conflict was undertaken in the FOIA rather than in the Privacy Act. The FOIA provides flexible exemptions from its disclosure requirements, especially exemption (b)(6), which protects information the disclosure of which would constitute a clearly

2187. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(3) (Supp. Feb. 1975).
2188. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(6) (Supp. Feb. 1975).
2189. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(5) (Supp. Feb. 1975).
2190. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(7) (Supp. Feb. 1975).
2191. Privacy Act § 3, 5 U.S.C.A. § 552a(k)(4) (Supp. Feb. 1975).
2192. *See* text at note 1934 *supra.*
2193. *See* text at notes 1990-93 *supra.*
2194. *See* text at notes 1536-49 *supra.*
2195. *See* text at notes 939-42 *supra.*

unwarranted invasion of personal privacy.[2196] These exemptions necessitate a balancing of conflicting interests and envision the dissemination to third parties of some types of information but not of other types. The Privacy Act, on the other hand, adopts a blanket approach that confers on the data subject control over the dissemination of all records (with certain rigid exceptions) without reference to the nature of the information they contain.[2197] In particular, the Privacy Act contains four provisions that together purport to exempt disclosures that are required under the FOIA from all of the dissemination restrictions in the Privacy Act. The intention, as indicated in the legislative history of the Privacy Act, was "to preserve the status quo as interpreted by the courts regarding the disclosure of personal information under [the FOIA]."[2198] The result, therefore, is that disclosure decisions are made under the FOIA rather than under the Privacy Act.

Subsection (b)(2) of the Privacy Act exempts agencies disclosing information under the FOIA from the obligation to obtain the data subject's written consent prior to dissemination. This exemption seems reasonable because it prevents individuals from frustrating legitimate FOIA requests. In order to facilitate data subject challenges to FOIA requests through reverse FOIA suits,[2199] however, the Privacy Act should have required that an individual be notified when an FOIA request is made for his file. Without such a notification requirement, the Act accords too little protection to privacy because agencies cannot be depended on to assert individual privacy interests vigorously. Subsection (c)(1) of the Privacy Act similarly exempts FOIA disclosures from the requirement that each agency keep accountings of the disseminations of each file. While it is possible that disclosure of the identities of FOIA requesters to data subjects might discourage some FOIA requests, that danger seems too remote to outweigh the subject's privacy interest in knowing how information about him is being disseminated.

Subsection (e)(6) of the Privacy Act exempts FOIA disclosures from its requirement that an agency make reasonable efforts to assure the accuracy of an individual file prior to dissemination. This exception does not change the procedures under the FOIA, which itself does not require that an agency disclose only accurate files. As the FOIA is intended to enable citizens to monitor the workings of government,[2200] such a requirement within the FOIA would be sub-

---

2196. *See generally* text at notes 700-44 *supra*.

2197. The Privacy Act drew its exemptions very specifically. No "balancing" decisions must be made to decide if a record is exempted. *Cf.* text at notes 496-500 *supra*.

2198. 120 CONG. REC. H12,244 (daily ed. Dec. 18, 1974).

2199. *See* text at notes 1132-67 *supra*.

2200. *See* text at note 2096 *supra*.

ject to attack on the ground that it would enable agencies to prevent citizens from discovering that improper information is being collected and maintained. This exemption in the Privacy Act should not present any serious dangers to privacy because of the protection provided by exemption six of the FOIA. The Privacy Act exemption perpetuates, however, the deficiencies, discussed above,[2201] associated with FOIA exemption six.

In the area of subject access, the interaction of the FOIA and the Privacy Act is delicate. In addition to the right of subject access contained in the Privacy Act, the principle underlying the FOIA of maximizing disclosure of agency records could provide a right of subject access in some situations, although the FOIA has not been so used in most of the litigation to date.[2202] There are limitations in both acts, however, on the right of subject access, and an agency desiring to avoid disclosure may well try to use the limitations in one act to bar subject access under both. Subsection (q) of the Privacy Act states that the FOIA exemptions may not be used to block subject access under the Privacy Act. The applicability of the Privacy Act subject access limitations to the FOIA, however, is dealt with only indirectly by subsection (b)(3) of the FOIA, which allows nondisclosure of information "specifically exempted from disclosure by statute."[2203] The question then is whether information exempted from subject access under the Privacy Act is "specifically exempted from disclosure" within the meaning of FOIA subsection (b)(3).

The Privacy Act exemptions, despite their grant of discretion to the heads of certain agencies to exempt certain records,[2204] are probably sufficiently specific to satisfy the terms of (b)(3).[2205] There are, however, two convincing arguments that (b)(3) does not incorporate the limitations on subject access contained in the Privacy Act. First, the Privacy Act does not literally require that certain records be kept confidential from the subject. Instead, it merely exempts certain records from its own subject access requirements. Although the Privacy Act does not contain an express provision authorizing subject access where specifically authorized by another statute, the Privacy Act should probably be so interpreted in light of its apparent policy in favor of subject access.

Second, if (b)(3) incorporates into the FOIA the Privacy Act limitations on subject access, then it must also incorporate all of the

---

2201. *See* text at notes 700-44 *supra*.

2202. *But see* Koch v. Department of Justice, 376 F. Supp. 313 (D.D.C. 1974), where the plaintiff was denied disclosure of FBI files concerning him. Representative Koch, the losing plaintiff there, was one of the leading sponsors of the Privacy Act. *See* 120 CONG. REC. H12,248 (daily ed. Dec. 18, 1974).

2203. 5 U.S.C. § 552(b)(3) (1970).

2204. Privacy Act § 3, 5 U.S.C.A. §§ 552a(j), (k) (Supp. Feb. 1975).

2205. *See* text at notes 568-610 *supra*.

disclosure limitations of the Privacy Act. This result flows from subsection (a)(3) of the FOIA, which has been interpreted to require that disclosures under the FOIA be made without reference to the identity of the requester.[2206] Information withheld from the data subject under the Privacy Act, therefore, could be withheld under (b)(3) from all requesters under the FOIA. An interpretation of (a)(3) to allow the withholding of information, under subsection (b)(3), from the data subject alone, would lead to the nonsensical result that data subjects would be barred from access to information available under the FOIA to third parties. Incorporation of the Privacy Act subject access limitations into the FOIA, via subsection (b)(3), would thus lead to the conclusion that despite its apparent intention not to alter the FOIA,[2207] Congress in effect amended the FOIA exemptions to be at least as broad as the Privacy Act exemptions. The result would be that all CIA files, for example, even if unclassified, would be exempted from the FOIA, as well as virtually all criminal investigatory files, despite the recent amendments narrowing subsection (b)(7) of the FOIA.

If the disclosure limitations of the Privacy Act are not incorporated into the FOIA via subsection (b)(3), data subjects could try to obtain access to their files under the FOIA wherever the FOIA exemptions are narrower than those in the Privacy Act, as they are with respect to criminal investigatory files. There are still several other obstacles, however, to subject access under the FOIA. For example, an agency might assert the (b)(6) exemption to the extent information in the file concerns the subject's private affairs. The subject should be able to overcome that obstacle with the very sensible argument that disclosure to him of information concerning his own private affairs would certainly not violate his privacy. This argument, however, violates the rule against taking into consideration the identity of the particular requester in applying the FOIA exemptions.[2208] Further, subject access might arguably constitute a waiver by the data subject of his right of privacy. Rejection of these formalistic arguments would be consistent with the proposal made above to employ balancing in deciding whether to release material covered by the (b)(6) exemption to the FOIA.[2209] Similar arguments could be used to circumvent the FOIA (b)(4) exemption for financial information,[2210] if it were employed to block subject access. One legitimate justification, however, for an agency denial of

2206. *See* note 458 *supra* and accompanying text.

2207. *See* text at note 2198 *supra*.

2208. *See* note 458 *supra* and accompanying text. In FOIA exemption six cases the courts have sometimes considered the identity and interests of the requester. *See* text at notes 716-34 *supra*.

2209. *See* text at notes 741-44 *supra*.

2210. 5 U.S.C. § 552(b)(4) (1970). *See* text at notes 611-47 *supra*.

subject access under the FOIA is the (b)(5) exemption for inter- and intra-agency memoranda.[2211]

The potential obstacles to subject access under the FOIA show that the Privacy Act's right of subject access—where applicable—improves the protection of privacy interests. With respect to the other privacy interests, such as being notified that a file is maintained, being able to challenge inaccurate or irrelevant information in one's file, and having control over inter-agency dissemination of the file, the Privacy Act, despite its deficiencies—especially its failure to control adequately inter-agency dissemination,[2212] its insufficient remedies to enforce the rights it creates,[2213] and its overbroad exemptions[2214]—clearly represents a major step toward satisfactory safeguards for individual privacy. There is need, however, for a clarification of the interaction of the Privacy Act and the FOIA. The best method of resolving current ambiguities would probably be to delineate within the Privacy Act the full scope of the right of subject access, and to make clear that the Privacy Act exemptions do not apply to the FOIA. The FOIA and Privacy Act exemptions need not be made uniform in all respects, but Congress should reexamine the exemptions in both acts to ensure that in no instance can a third party obtain access to a file under the FOIA where the Privacy Act denies access to the subject.

2211. 5 U.S.C. § 552(b)(5) (1970). *See* text at notes 648-99 *supra*. This exemption was used to deny access in Koch v. Department of Justice, 376 F. Supp. 313, 316 (D.D.C. 1974).

2212. *See* text at notes 2107-28 *supra*.

2213. *See* text at notes 2129-62 *supra*.

2214. *See* text at notes 2163-95 *supra*.

Appendix C

Analysis of Selected Cases Decided Under the Sixth Exemption of the Freedom of Information Act Apropos the Right of Privacy of Affected Individuals Against the Right of the Public to Be Informed

(By Paul S. Wallace, Jr., Legislative Attorney, Congressional Research Service)

The Freedom of Information Act (5 U.S.C. § 552) states generally that each Federal agency shall make available to the public certain specified information. Section 552(b)(1-9) of Title 5 represents a recognition by Congress that "certain information in Government files" should be exempt from disclosure. S. Rept. 813, 89th Cong., 1st Sess., 3 (1965). While the cases involving Exemption (6) are numerous, every effort was made to include only those cases which construe by definitive analysis the provisions of the exemption. Exemption (6) protects from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6) (1970 ed.).

The *Senate* and *House Reports* noted that agencies like the Veterans' Administration, Department of Health, Education, and Welfare, Selective Service, etc., have great quantities of files containing intimate details about millions of citizens. See S. Rept. No. 813, 89th Cong., 1st Sess., 9 (1966); H.R. Rept. No. 1497, 89th Cong., 2d Sess., 11 (1966). Congressional awareness of possible conflicts between the right of the public to know and the intrusion into individual privacy would appear to be the reason for the creation of exemption (6) as the primary balancing machinery

The *House Report* states:

"A general exemption for the category of information is much more practical than separate statutes protecting each type of personal record. The limitation of a 'clearly unwarranted invasion of personal privacy' provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to Government information by excluding those kinds of files the disclosure of which might harm the individual. The exemption is also intended to cover detailed Government records on an individual which can be identified as applying to that individual and not the facts concerning the award of a pension or benefit or the compilation of unidentified statistical information from personal records." H. Rept. No. 1497, 89th Cong., 2d Sess. 11 (1966).

The *Senate Report* states:

"At the same time that a broad philosophy of 'freedom of information' is enacted into law, it is necessary to protect certain equally important rights of privacy with respect to certain information in Government files, such as medical and personnel records. It is also necessary for the very operation of our Government to allow it to keep confidential certain material, such as the investigatory files of the Federal Bureau of Investigation.

"It is not an easy task to balance the opposing interests, but it is not an impossible one either. It is not necessary to conclude that to protect one of the interests, the other must, of necessity, either be abrogated or substantially subordinated. Success lies in providing a workable formula which encompasses, balances, and protects all interests, yet places emphasis on the fullest responsible disclosure." S. Rept. No. 813, 89th Cong., 1st Sess. 3 (1966).

Professor Davis takes the position that balancing was not intended under the Act. The requests of all information seekers are equal since the provision of former section 3 providing for disclosure was changed from "to persons properly and directly concerned" to "to any person." K. Davis, Administrative Law Treatise, Sec. 3A. 4, p. 120 (1970 Supp.).

In one of the earlier cases decided under the Act, the Court of Appeals for the District of Columbia in *Ackerley* v. *Ley*, 420 F. 2d 1336, 1339-40 (D.C. Cir. 1969), stated in dictum that medical files received under a pledge of confidentiality cannot, in and of itself, justify nondisclosure under Exemption 6, even though the records are explicitly mentioned in it and are the kind which the exeption intended to protect from disclosure In another case, *Robles* v. *Environmental Protection Agency*, 484 F. 2d 843, 848 (4th Cir. 1973), the court, applying a general public interest standard as against weighing the interest of the particular individual obtaining the information, held that plaintiff's interest in surveys dealing with the existence of uranium trailings found in foundations of

individual homes may provide a beneficial, calming effect on the reasonable apprehensions of citizens and would override any interest of privacy that the individual home owners had in not disclosing it. The court stated that the right to disclosure under the Act is not to be resolved by a balancing of equities or a weighing of need or benefit; the only ground for denial of disclosure here is that the disclosure would represent a "clearly unwarranted invasion of personal privacy." *Ibid.*, at 848.

In *Getman* v. *National Labor Relations Board*, 450 F. 2d 670 (D.C. Cir. 1971) and *Wine Hobby, U.S.A., Inc.* v. *United States Bureau of Alcohol, Tobacco, and Firearms*, 363 F. Supp. 231 (E.D. Pa. 1973), rev'd 502 F. 2d 133 (3d Cir. 1974), the courts interpreted Exemption 6 as requiring "a court reviewing the matter *de novo* to balance the right of privacy of affected individuals against the right of the public to be informed." 450 F. 2d at 674; 502 F. 2d at 136. In *Getman*, lists containing names and addresses of employees eligible to vote in certain representation elections were requested by two labor law professors. The requesters had planned to communicate with the employees appearing on the list in order to evaluate the voting regulations of the NLRB. 450 F. 2d at 671–72. The court ruled in favor of disclosure after concluding that the invasion of privacy was "very minimal" and that the study could benefit the public significantly. 450 F. 2d at 677. However, in *Wine Hobby* where the requester stipulated that it sought the information for "private commercial exploitation", the court denied the release of the information in light of the requester's failure to assert a public interest purpose for disclosure. 502 F. 2d at 137. The court concluded that the "invasion of privacy caused by disclosure would be 'clearly unwarranted', even though the invasion of privacy in this case [was] not as serious as that considered by the court in other cases." *Ibid.*

In *Tuchinsky* v. *Selective Service System*, 294 F. Supp. 803, 804 (N.D. Ill. 1969), aff'd 418 F. 2d 155 (7th Cir. 1969), the court held that a draft counselor was entitled to the names of the local Selective Service Board officials, but was not entitled to personal information in regard to such matters as their home addresses, occupations, races, dates of appointment, military affiliations, and citizenship, under the Freedom of Information Act, in view of a Selective Service regulation permitting the release of personal information only "if the person involved consents, and the local board chairman, after consultation with the person involved, determines in writing that disclosures would not harm that person and would not be a clearly unwarranted invasion of that person's personal privacy."

The 1967 *Attorney General's Memorandum* does not set forth any guidelines for determining what constitutes an invasion of personal privacy; however, it referred to the *House Report* which "noted that the Civil Service Commission . . . ruled that 'the names, position titles, grades, salaries, and duty stations of Federal employees are public information'." *U.S. Dept. of Justice Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act* (1967) 37. The memorandum concludes by stating that "whether such addresses are protected by this exemption would depend upon the context in which they are sought." *Ibid.*

In balancing interests, the courts have considered in their determination of whether there may be an invasion of privacy, the extent of the invasion of privacy, the public interest that would be served by disclosure, whether the interest could be satisfied without the requested materials, see *Getman* v. *NLRB*, 450 F. 2d 670, 674–75 (D.C. Cir. 1971); *Rural Housing Alliance* v. *Department of Agriculture*, 498 F. 2d 73, 77–78 (D.C. Cir. 1974), whether the material is available elsewhere, see *Rural Housing Alliance* v. *Department of Agriculture*, 489 F. 2d 73, 78 (D.C. Cir. 1974); *Ditlow* v. *Shultz*, 379 F. Supp. 326, 331–32 (D.D.C. 1974), promises of confidentiality, see *Robles* v. *EPA*, 484 F. 2d 843, 846 (4th Cir. 1973), and whether the affected individual is willing to give permission to release the information, see *Rural Housing Alliance* v. *Department of Agriculture*, 498 F. 2d 73, 82–83 (D.C. Cir. 1974).

Similar to *Robles* v. *EPA*, the court in *Rose* v. *Department of the Air Force*, 495 F. 2d 261 (2d Cir. 1974) cert. granted 43 U.S.L.W. 3451 (Feb. 18, 1975) (No. 74-489), appeared to have considered the seriousness of the intrusion on the individual privacy rather than balancing that intrusion on the individual with the public interest which would be served as a result of the disclosure.

In *Rose*, the United States Court of Appeals for the Second Circuit held that the Air Force Academy Cadet Honor and Ethics Code case summaries were not

exempt from disclosure under Exemption (6). In addition, the court refused to deny disclosure of the case summaries by utilizing a broad power of equitable discretion to prevent harm to the public interest. 495 F. 2d at 269.

Expressing its primary concern for privacy, the *Rose* court set forth a basis upon which each potential privacy intrusion will be evaluated:

"Each case involves an essentially unique investigation into the nature of the privacy interest invaded and the extent of the proposed invasion, viewed in the light of contemporary mores and sensibilities as applied to the particular facts." *Ibid.* at 266.

Although the court concluded that the case summaries, all or in part, were not protected from disclosure by Exemption (6), this conclusion did not affect the Court's primary concern for privacy. On remand, the district court was instructed to delete all personal references and all other identifying information and "if, in the opinion of the district judge, this [was] not sufficient to safeguard privacy, then the summaries should not be disclosed . . . *Ibid*, at 268.

By accepting *Rose* v. *Department of Air Force* for review, the Supreme Court will have before it the following questions under Exemption 6:

"Whether Exemption (6) covers all personnel files rather than only those whose disclosure 'would constitute a clearly unwarranted invasion of personal privacy'?

"Whether the exemption bars disclosure of summaries of proceedings against cadets at Air Force Academy accused of violation of Honor and Ethics Codes, because such disclosure 'would constitute a clearly unwarranted invasion of personal privacy'?" 44 U.S.W. 3017 (July 22, 1975).

CONCLUSION

The legislative history appears to support use of the balancing test in the treatment of Exemption (6) issues. Consequently, the agencies and the reviewing courts have the responsibility to determine the point where the public's need for information no longer outweighs the individual's invasion of privacy. In applying the balancing test in *Getman*, the court considered such factors as the extent of the invasion of privacy, the public interest that would be served by disclosure, and whether the interest could be satisfied without the requested material in its efforts to accommodate both the right to privacy and the right to information. The *Rose* case restricted the discretionary balancing approach in *Getman* by concentrating on the element of privacy in its determination of whether the invasion of privacy was "clearly unwarranted." Since a majority of the cases indicate that the courts are sensitive to the concept of personal privacy, it would appear that if a request involves this exemption, a brief explanation of why the information is needed would be helpful so that it can be determined whether the invasion of privacy resulting from disclosure would be "unwarranted."

[From the United States Law Week, 44 LW 4503, Apr. 20, 1976]

DEPARTMENT OF THE AIR FORCE ET AL., PETITIONERS

v.

MICHAEL T. ROSE ET AL.

No. 74–489

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

[April 21, 1976]

SYLLABUS

Under the United States Air Force Academy's Honor Code, which is administered by a cadet committee, cadets pledge that they will not lie, steal, or cheat, or tolerate among their number anyone who does. If a cadet investigatory team finds that a hearing concerning a suspected violation is warranted, the accused may call witnesses, and cadet observers attend. An eight-man Honor Board

may adjudge guilt only by unanimous vote but may if at least six members concur grant the guilty cadet "discretion," which returns him to his squadron in good standing. A cadet found guilty without discretion may resign, or request a hearing by officers or trial by court-martial. The hearing is confidential but the committee prepares a summary, which is posted on 40 squadron bulletin boards and distributed among Academy faculty and officials. In not-guilty and discretion cases, names are deleted. In guilty cases names are not deleted but posting is deferred until the cadet has left the Academy. Ethics Code violations, for less serious breaches, are handled more informally, though on a similarly confidential basis. Respondents, present or former student law review editors researching for an article, having been denied access to case summaries of honors and ethics hearings (with identifying data deleted), brought this suit to compel disclosure under the Freedom of Information Act (FOIA) against the Department of the Air Force and certain Academy officers (hereinafter collectively the "Agency"). The District Court without *in camera* inspection granted the Agency's motion for summary judgment on the ground that the summaries were "matters . . . related solely to the internal personnel rules and practices of an agency," and thus exempted from mandatory disclosure under Exemption 2 of the FOIA. The Court of Appeals reversed, holding that exemption inapplicable. The Agency had made the contention, which the District Court rejected, that the case summaries fell within Exemption 6 as constituting "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy." The Court of Appeals, while disagreeing with the District Court's approach, did not hold that the Agency without any prior court inspection had to turn over the summaries to respondents with only the proper names removed or that Exemption 6 covered all or any part of the summaries, but held that because the Agency had not maintained its statutory burden in the District Court of sustaining its action by means of affidavits or testimony further inquiry was required and that the Agency had to produce the summaries for an *in camera* inspection, cooperating with the District Court in redacting the records so as to delete personal reference and all other identifying information. *Held:*

1. The limited statutory exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant legislative objective of the FOIA.

2. Exemption 2 does not generally apply to matters, such as the summaries here involved, in which there is a genuine and important public interest.

(a) The phrasing of that exemption reflected congressional dissatisfaction with the "internal management" exemption of former § 3 of the Administrative Procedure Act and was generally designed, as the Senate Report made clear, to delineate between, on the one hand, trivial matters and, on the other, more substantial matters in which the public might have a legitimate interest.

(b) The public has a substantial concern with the Academy's administration of discipline and procedures that affect the training of Air Force officers and their military careers.

3. Exemption 6 does not create a blanket exemption for personnel files. With respect to such files and "similar files" Congress enunciated a policy, to be judicially enforced, involving a balancing of public and private interests. Regardless of whether the documents whose disclosure is sought are in "personnel" or "similar" files, nondisclosure is not sanctioned unless there is a showing of a clearly unwarranted invasion of personal privacy, and redaction of documents to permit disclosure of nonexempt portions is appropriate under Exemption 6.

4. Even if "personnel files" were to be considered as wholly exempt from disclosure under Exemption 6 without regard to whether disclosure would constitute a clearly unwarranted invasion of personel privacy, the case summaries here were not in that category although they constituted "similar files" relating as they do to the discipline of cadets, and their disclosure implicating similar privacy values.

5. The Court of Appeals did not err in ordering the Agency to produce the case summaries for the District Court's *in camera* examination, a procedure that represents "a workable compromise between individual rights and the preservation of public rights to [G]overnment information.'" which is the statutory goal of Exemption 6.

(a) The limitation in Exemption 6 to cases of "clearly unwarranted" invasions of privacy indicates that Congress did not intend a matter to be exempted from disclosure merely because it could not be guaranteed that disclosure would not trigger recollection of identity in any person whatever, and

Congress vested the courts with the responsibility of determining *de novo* whether the exemption was properly invoked.

(b) Respondents' request for access to summaries "with personal references or other identifying information deleted" respected the confidentiality interests embodied in Exemption 6 and comported with the Academy's tradition of confidentiality.

495 F.2d 261, affirmed.

Brennan, J., delivered the opinion of the Court, in which Stewart, White, Marshall, and Powell, JJ., joined. Burger, C. J., and Blackmun and Rehnquist, JJ., filed dissenting opinions. Stevens, J., took no part in the consideration or decision of the case.

Mr. Justice Brennan delivered the opinion of the Court.

Respondents, student editors or former student editors of the New York University Law Review researching disciplinary systems and procedures at the military service academies for an article for the Law Review,[1] were denied access by petitioners to case summaries of honor and ethics hearings, with personal references or other identifying information deleted, maintained in the United States Air Force Academy's Honor and Ethics Code Reading Files, although Academy practice is to post copies of such summaries on 40 squadron bulletin boards throughout the Academy and to distribute copies to Academy faculty and administration officials.[2] Thereupon respondents brought this action under the Freedom of Information Act, as amended, 5 U.S.C. § 552, in the District Court for the Southern District of New York against petitioners, the Department of the Air Force and Air Force officers who supervise cadets at the United States Air Force Academy (hereinafter collectively the "Agency").[3] The District

---

[1] Respondent Michael T. Rose, a graduate of the United States Air Force Academy and at that time a First Lieutenant in the Air Force, was the student editor charged with preparing the study. It finally appeared as a book, Rose, "A Prayer for Relief: The Constitutional Infirmities of the Military Academies' Conduct, Honor and Ethics Systems" (NYU 1973). Respondents Lawrence P. Pedowitz and Charles P. Diamond were, at the time this suit was filed, respectively the former and current Editor-in-Chief of the Review.

[2] Upon respondent Rose's request for documents, Academy officials gave him copies of the Honor Code, the Honor Reference Manual, Lesson Plans, Honor Hearing Procedures, and various other materials explaining the Honor and Ethics Codes. They denied him access to the case summaries, however, on the grounds that even with the names deleted "[s]ome cases may be recognized by the reader by the circumstances alone without the identity of the cadet given" and "[t]here is no way of determining just how these facts will or could be used." App. 21, 155, 157, 184, 186. On appeal to the Secretary of the Air Force, the Secretary, by letter from his Administrative Assistant, refused disclosure of the case summaries on the ground that they were exempt from disclosure by Exemption 6, 5 U.S.C. § 522 (b)(6), of the Freedom of Information Act and by Air Force Regulations 12–30 ¶¶ 4 (f) and 4 (g)(1)(b), 32 CFR §§ 806.5 (f), (g)(1)(ii), App. 21, 121–122.

[3] The Freedom of Information Act, 5 U.S.C. § 552, as amended, Public Law 93–502, 88 Stat. 1561, provides in pertinent part:

"(a) Each agency shall make available to the public information as follows:

* * * * * * *

"(3) Except with respect to the records made available under paragraphs (1) and (2) of this section, each agency, upon any request for records which (A) reasonably describes such records and (B) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

"(4) (A). . . .

"(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action.

* * * * * * *

"(b) This section does not apply to matters that are—

* * * * * * *

"(2) related solely to the internal personnel rules and practices of an agency;

* * * * * * *

"(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

* * * * * * *

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.

"(c) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. . . ."

Court granted petitioner Agency's motion for summary judgment—without first requiring production of the case summaries for inspection—holding in an unreported opinion that case summaries even with deletions of personal references or other identifying information were "matters . . . related solely to the internal personnel rules and practices of an agency," exempted from mandatory disclosure by § 552(b)(2) of the statute.[4] The Court of Appeals for the Second Circuit reversed, holding that § 552(b)(2) did not exempt the case summaries from mandatory disclosure. 495 F.2d 261 (1974). The Agency argued alternatively, however, that the case summaries constituted "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," exempted from mandatory disclosure by § 552(b)(6).

The District Court held this exemption inapplicable to the case summaries, because it concluded that disclosure of the summaries without names or other identifying information would not subject any former cadet to public identification and stigma, and the possibility of identification by another former cadet could not, in the context of the Academy's practice of distribution and official posting of the summaries, constitute an invasion of personal privacy proscribed by § 552(b)(6). Petition for Certiorari, at 32A. The Court of Appeals disagreed with this approach, stating that it "ignores certain practical realities" which militated against the conclusion "that the Agency's internal dissemination of the summaries lessens the concerned cadets' right to privacy, as embodied in Exemption 6." 495 F. 2d, at 267. But the Court refused to hold, on the one hand, either "that [the Agency] must now, without any prior inspection by a court, turn over the summaries to [respondents] with only the proper names removed . . ." or, on the other hand, "that Exemption Six covers all, or any part of, the summaries in issue." *Id.*, at 268. Rather, the Court of Appeals held that because the Agency had not carried its burden in the District Court, imposed by the Act, of "sustain[ing] its action" by means of affidavits or testimony, further inquiry was required, and "the Agency must produce the summaries themselves in court" for an *in camera* inspection "and cooperate with the judge in redacting the records so as to delete personal references and all other identifying information. . . . We think it highly likely that the combined skills of court and Agency, applied to the summaries, will yield edited documents sufficient for the purpose sought and sufficient as well to safeguard affected persons in their legitimate claims of privacy." *Ibid.*

We granted certiorari, 420 U.S. 923 (1975). We affirm.

I

The District Court made factual findings respecting the administration of the Honor and Ethics Codes at the Academy. See Petition for Certiorari, at 28A–29A nn. 5, 6. Under the Honor Code enrolled cadets pledge that "We will not lie, steal, or cheat, nor tolerate among us anyone who does." The Honor Code is administered by an Honor Committee composed of Academy cadets. Suspected violations of the Code are referred to the Chairman of the Honor Committee, who appoints a three-cadet investigatory team which, with advice from the legal advisor, evaluates the facts and determines whether a hearing, before a Board of eight cadets, is warranted. If the team finds no hearing warranted, the case is closed. If it finds there should be a hearing, the accused cadet may call witnesses to testify in his behalf, and each cadet squadron may ordinarily send two cadets to observe.

The Honor Board may return a guilty finding only upon unanimous vote. If the verdict is guilty, under certain circumstances the Board may grant the guilty cadet "discretion," for which a vote of 6 of the 8 members is required. A verdict of guilty with discretion is equivalent to a not guilty finding in that the cadet

---

[4] Respondents also sought access to a complete study of resignations of Academy graduates from the Air Force. Petitioners claimed that the study was exempted from disclosure by § 522 (b)(2)(5) of the Freedom of Information Act, 5 U.S.C. § 552 (b)(5), concerning "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." The District Court held that since the study had already been offered for dissemination to the public the Agency had waived its rights under the exemption, and accordingly it granted respondents partial summary judgment, requiring petitioners to disclose the complete study to respondents. Petition for Certiorari, at 35A–38A. Petitioners compiled with this order.

is returned to his cadet squadron in good standing. A verdict of guilty without discretion results in one of three alternative dispositions: the cadet may resign from the Academy, request a hearing before a Board of Officers, or request a trial by court-martial.

At the announcement of the verdict, the Honor Committee Chairman reminds all cadets present at the hearing that all matters discussed at the hearing are confidential and should not be discussed outside the room with anyone other than an Honor Representative. A case summary consisting of a brief statement, usually only one page, of the significant facts is prepared by the Committee. As we have said, copies of the summaries are posted on 40 squadron bulletin boards throughout the Academy, and distributed among Academy faculty and administration officials. Cadets are instructed not to read the summaries, unless they have a need, beyond mere curiosity, to know their contents, and the Reading Files are covered with a notice that they are "for official use only." Case summaries for not guilty and discretion cases are circulated with names deleted; in guilty cases, the guilty cadet's name is not deleted from the summary, but posting on the bulletin boards is deferred until after the guilty cadet has left the Academy.

Ethics Code violations are breaches of conduct less serious than Honor Code violations, and administration of Ethics Code cases is generally less structured, though similar. In many instances, Ethics cases are handled informally by the Cadet Squadron Commander, the Squadron Ethics Representative, and the individual concerned. These cases are not necessarily written up and no complete file is maintained; a case is written up and the summary placed in back of the Honor Code Reading Files only if it is determined to be of value for the Cadet population. Distribution of Ethics Code summaries is substantially the same as that of Honor Code summaries, and their confidentiality, too, is maintained by Academy custom and practice.

II

Our discussion may conveniently begin by again emphasizing the basic thrust of the Freedom of Information Act. We canvassed the subject at some length three years ago in *Environmental Protection Agency* v. *Mink*, 410 U.S. 73, 79–80 (1973), and need only briefly review that history here. The Act revises § 3, the public disclosure section, of the Administrative Procedure Act, 5 U.S.C. § 1002 (1964). The revision was deemed necessary because "Section 3 was generally recognized as falling far short of its disclosure goals and came to be looked upon more as a withholding statute than a disclosure statute." *Mink*, *supra*, at 79. Congress therefore structured a revision whose basic purpose reflected "a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." S. Rep. No. 813, 89th Cong., 1st Sess., at 3 (1965) (hereinafter S. Rep. No. 813). To make crystal clear the congressional objective—in the words of the Court of Appeals, "to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny," 495 F. 2d, at 263—Congress provided in § 552(c) that nothing in the Act should be read to "authorize withholding of information or limit the availability or records to the public, except as specifically stated. . . ."

Consistently with that objective, the Act repeatedly states "that official information shall be made available 'to the public,' 'for public inspection.'" *Mink*, *supra*, at 79. There are, however, exemptions from compelled disclosure. They are nine in number and are set forth in § 552(b). But these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act. "These exemptions are specifically made exclusive, 5 U.S.C. § 522(c) . . . ." *Mink*, *supra*, at 79, and must be narrowly construed. *Vaughn* v. *Rosen*, 157 U.S. App. D.C. 340, 343, 484 F. 2d 820, 823 (1973). — U.S. App. D.C. —, —, — F. 2d — (1975), No. 75–1031, Nov. 21, 1975, slip op. at 422; *Soucie* v. *David*, 145 U.S. App. D.C. 144, 157, 448 F. 2d 1067, 1080 (1971). In sum, as said in *Mink* *supra*, at 80:

"Without question, the Act is broadly conceived. It seeks to permit access to official information long shielded unnecessarily from public view and attempts to create a judicially enforceable public right to secure such information from possibly unwilling official hands. Subsection (b) is part of this scheme and represents the congressional determination of the types of information that the Executive Branch must have the option to keep confidential, if it so chooses. As the Senate Committee explained, it was not 'an easy task to balance the opposing

interests, but it is not an impossible one either. . . . Success lies in providing a workable formula which encompasses, balances, and protects all interests, yet places emphasis on the fullest responsible disclosure.' S. Rep. No. 813, p. 3."

Mindful of the congressional purpose, we then turn to consider whether mandatory disclosure of the case summaries is exempted by either of the exemptions involved here, discussing *first* Exemption 2, and *second* Exemption 6.

III

The phrasing of Exemption 2 is traceable to congressional dissatisfaction with the exemption from disclosure under former § 3 of the Administrative Procedure Act of "any matter relating solely to the internal management of an agency." 5 U.S.C. § 1002 (1964). The sweep of that wording led to withholding by agencies from disclosure of matter "rang[ing] from the important to the insignificant." H. H. Rep. No. 1497, 89th Cong., 2d Sess., at 5 (1966) (hereinafter H. R. Rep. No. 1497). An earlier effort at minimizing this sweep, S. 1666 introduced in the 88th Congress in 1963, applied the "internal management" exemption only to matters required to be published in the Federal Register; agency orders and records were exempted from other public disclosure only when the information related "solely to the internal personnel rules and practices of any agency." The distinction was highlighted in the Senate Report on S. 1666 by reference to the latter as the "more tightly drawn" exempting language. S. Rep. No. 1219, 88th Cong., 2d Sess., 12.

No final action was taken on S. 1666 in the 88th Congress; the Senate passed the Bill, but it reached the House too late for action. *Renegotiation Board* v. *Bannercraft Clothing Co.*, 415 U.S. 1, 18 n. 18 (1974). But the Bill introduced in the Senate in 1965 that became law in 1966 dropped the "internal management" exemption for matters required to be published in the Federal Register and consolidated all exemptions into a single subsection. Thus, legislative history plainly evidences the congressional conclusion that the wording of Exemption 2, "internal personnel rules and practices," was to have a narrower reach than the Administrative Procedure Act's exemption for "internal management."

But that is not the end of the inquiry. The House and Senate Reports on the Bill finally enacted differ upon the scope of the narrowed exemption. The Senate Report stated: "Exemption 2 relates only to the internal personnel rules and practices of an agency. Examples of these may be rules as to personnel's use of parking facilities or regulations of lunch hours, statements of policy as to sick leave, and the like." S. Rep. No. 813, at 8.

The House Report, on the other hand, declared:

"'2. Matters related solely to the internal personnel rules and practices of any agency. Operating rules, guidelines and manuals of procedure for Government investigators or examiners would be exempt from disclosure but this exemption would not cover all 'matters of internal management' such as employee relations and working conditions and routine administrative procedures which are withheld under the present law." H.R. Rep. No. 1497, at 10.

Almost all courts that have considered the difference between the Reports have concluded that the Senate Report more accurately reflects the congressional purpose.[5] Those cases relying on the House, rather than the Senate, interpretation of Exemption 2, and permitting Agency withholding of matters of some public interest, have done so only where necessary to prevent the circumvention of agency regulations that might result from disclosure to the subjects of regulation of the procedural manuals and guidelines used by the agency in discharging its regulatory function. See, *e.g.*, *Tietze* v. *Richardson*, 342 F. Supp. 610 (SD Tex. 1972); *Cuneo* v. *Laird*, 338 F. Supp. 504 (DC 1972); rev'd on other grounds, *sub. nom. Cuneo* v. *Schlesinger*, 157 U.S. App. D.C. 368, 484 F. 2d 1086; *City of Concord* v. *Ambrose*, 333 F. Supp. 958 (ND Cal. 1971) (dictum). Moreover, the legislative history indicates that this was the primary concern of the committee drafting the House Report. See Hearings on H.R. 5012 before a Subcomm. of the House Comm. on Government Operations, 89th Cong., 1st Sess., 29–30 (1965).

---

[5] *E.g.*, *Stokes* v. *Brennan*, 476 F.2d 699, 703 (CA5 1973); *Hawkes* v. *IRS*, 467 F.2d 787, 796 (CA6 1972); *Stern* v. *Richardson*, 367 F. Supp. 1316, 1320 (DC 1973); *Consumers Union of United States, Inc.* v. *Veterans Administration*, 301 F. Supp. 796, 801 (SDNY 1969), appeal dismissed as moot, 436 F.2d 1363 (CA2 1971); *Benson* v. *GSA*, 289 F. Supp. 590, 595 (WD Wash. 1968), aff'd, 415 F.2d 878 (CA9 1969) (Exemption 2 apparently not raised on appeal).

cited in H.R. Rep. No. 1497, at 10 n. 14. We need not consider in this case the applicability of Exemption 2 in such circumstances, however, because, as the Court of Appeals recognized, this is not a case "where knowledge of administrative procedures might help outsiders to circumvent regulations or standards. Release of the [sanitized] summaries, which constitute quaisilegal records, poses no such danger to the effective operation of the Codes at the Academy." 495 F. 2d, at 265 (footnote omitted). Indeed, the materials sought in this case are distributed to the subjects of regulation, the cadets, precisely in order to assure their compliance with the known content of the Codes.

It might appear, nonetheless, that the House Report's reference to "[o]perating rules, guidelines, and manuals of procedure" supports a much broader interpretation of the exemption than the Senate Report's circumscribed examples. This argument was recently considered and rejected by Judge Wilkey speaking for the Court of Appeals of the District of Columbia Circuit in *Vaughn* v. *Rosen*, — U.S. App. D.C. —, —, 523, F. 2d 1136, 1142 (1975):

"Congress intended that Exemption 2 be interpreted narrowly and specifically. In our view, the House Report carries the potential of exempting a wide swath of information under the category of 'operating rules, guidelines, and manuals of procedure. . . .' The House Report states that the exemption 'would not cover all "matters of internal management" such as employee relations and working conditions and routine administrative procedures. . . .' and yet it gives precious little guidance as to which matters are covered by the exemption and which are not. Although it is equally terse, the Senate Report indicates that the line sought to be drawn is one between minor or trivial matters and those more substantial matters which might be the subject of legitimate public interest.

"This is a standard, a guide, which an agency and then a court, if need be, can apply with some certainty, consistency and clarity. . . .

"Reinforcing this interpretation is 'the clear legislative intent [of FOIA] to assure public access to all governmental records whose disclosure would not significantly harm specific governmental interests.' [*Soucie* v. *David*, 145 U.S. App. D. C. 144, 157, 448 F. 2d 1067, 1080 (1971).] As a result, we have repeatedly stated that '[t]he policy of the Act requires that the disclosure requirements be construed broadly, the exemptions narrowly.' [*Ibid; Vaughn* v. *Rosen*, 157 U.S. App. D.C. 340, 343, 484 F. 2d 820, 823.] Thus, faced with a conflict in the legislative history, the recognized principal purpose of the FOIA requires us to choose that interpretation most favoring disclosure.

"The second major consideration favoring reliance upon the Senate Report is the fact that it was the only committee report that was before both houses of Congress. The House unanimously passed the Senate Bill without amendment, therefore no conference committee was necessary to reconcile conflicting provisions. . . .

". . . [W]e as a court viewing the legislative history must be wary of relying upon the House Report, or even the statements of House sponsors, where their views differ from those expressed in the Senate. As Professor Davis said: 'The basic principle is quite elementary: The content of the law must depend upon the intent of both Houses, not of just one.' [*See generally*, K. Davis, *Administrative Law Treatise*, § 3A.31 (1970 Supp.) at 175.] By unanimously passing the Senate Bill without amendment, the House denied both the Senate Committee and the entire Senate an opportunity to object (or concur) to the interpretation written into the House Report (or voiced in floor colloquy). This being the case, we choose to rely upon the Senate Report."

For the reasons stated by Judge Wilkey, and because we think the primary focus of the House Report was on exemption of disclosures that might enable the regulated to circumvent agency regulation, we too "choose to rely upon the Senate report" in this regard.

The District Court had also concluded in this case that the Senate Report was "the surer indication of congressional intent." Petition for Certiorari, at 3a n. 21. The Court of Appeals found it unnecessary to take "a firm stand on the issue," concluding that "the difference of approach between the House and Senate Reports would not affect the result here." 495 F. 2d, at 265. The different conclusions of the two courts in applying the Senate Report's interpretation centered upon a disagreement as to the materiality of the public significance of the operation of the Honor and Ethics Codes. The District Court based its conclusion on a determination that the Honor and Ethics Codes "[b]y definition . . . are meant to control only those people in the agency. . . . The

operation of the Honor Code cannot possibly affect anyone outside its sphere of voluntary participation which is limited by its function and its publication to the Academy." Petition for Certiorari, at 34A. The Court of Appeals on the other hand concluded that under "the Senate construction of Exemption Two, [the] case summaries . . . clearly fall outside its ambit" because "[s]uch summaries have substantial potential for public interest outside the Government." 495 F. 2d, at 265.

We agree with the approach and conclusion of the Court of Appeals. The implication for the general public of the Academy's administration of discipline is obvious, particularly so in light of the unique role of the military. What we have said of the military in other contexts has equal application here: it "constitutes a specialized community governed by a separate discipline from that of the civilian," *Orloff* v. *Willoughby*, 345 U.S. 83, 94 (1953), in which the internal law of command and obedience invests the military officer with "a particular position of responsibility." *Parker* v. *Levy*, 417 U.S. 733, 744 (1974). Within this discipline, the accuracy and effect of a superior's command depends critically upon the specific and customery reliability of subordinates, just as the instinctive obedience of subordinates depends upon the unquestioned specific and customary reliability of the superior.[6] The importance of these considerations to the maintenance of a force able and ready to fight effectively renders them undeniably significant to the public role of the military. Moreover, the same essential integrity is critical to the military's relationship with its civilian direction. Since the purpose of the Honor and Ethics Codes administered and enforced at the Air Force Academy is to ingrain the ethical reflexes basic to these responsibilities in future Air Force officers, and to select out those candidates apparently unlikely to serve these standards, it follows that the nature of this instruction—and its adequacy or inadequacy—is significantly related to the substantive public role of the Air Force and its Academy. Indeed, the public's stake in the operation of the Codes as they affect the training of future Air Force officers and their military careers is underscored by the Agency's own proclamations of the importance of cadet-administered Codes to the Academy's educational and training program. Thus, the Court of Appeals said, and we agree:

"[Respondents] have drawn our attention to various items such as newspaper excerpts, a press conference by an Academy officer and a White House Press Release, which illustrate the extent of general concern with the working of the Cadet Honor Code. As the press conference and the Press Release show, some of the interest has been generated—or at least enhanced—by acts of the Government itself. Of course, even without such official encouragement, there would be interest in the treatment of cadets, whose education is publicly financed and who furnish a good portion of the country's future military leadership. Indeed, all sectors of our society, including the cadets themselves, have a stake in the fairness of any system that leads, in many instances, to the forced resignation of some cadets. The very study involved in this case bears additional witness to the degree of professional and academic interest in the Academy's student-run system of discipline. . . . [This factor] differentiate[s] the summaries from matters of daily routine like working hours, which, in the words of Exemption Two, do relate '*solely* to the internal personnel rules and practices of an agency' " 495 F. 2d, at 265 (emphasis in Court of Appeals opinion).

In sum, we think that, at least where the situation is not one where disclosure may risk circumvention of agency regulation, Exemption 2 is not applicable to matters subject to such a genuine and significant public interest. The exemption was not designed to authorize withholding of all matters except otherwise secret law bearing directly on the propriety of actions of members of the public. Rather, the general thrust of the exemption is simply to relieve agencies of the burden of assembling and maintaining for public inspection matter in which the public could not reasonably be expected to have an interest.[7] The case summaries plain-

---

[6] The Honor Reference Handbook of the Air Force Cadet Wing at 1, App., at 47, recites: "Former Secretary of War, Newton Baker, said, '. . . the inexact or untruthful soldier trifles with the lives of his fellow men and with the honor of his government. . . .' The young officer needs to be able to trust his men as does any commander. In these times of expensive and increasingly complex weapons systems, the officer must rely on fellow officers and airmen for his own safety and the safety of his men."

[7] See, *e.g.*, Note, the Freedom of Information Act: A Seven-Year Assessment, 74 Colum. L. Rev. 895, 956 (1974); Note, Comments on Proposed Amendments to Section 3 of the Administrative Procedure Act: The Freedom of Information Bill, 40 Notre Dame Law. 417, 445 (1955). See also *Vaughn* v. *Rosen*, — U.S. App. D.C. —, —, 523 F.2d 1136, 1150 (1975) (Leventhal, J., concurring).

ly do not fit that description. They are not matter with merely internal significance. They do not concern only routine matters. Their disclosure entails no particular administrative burden. We therefore agree with the Court of Appeals that, given the Senate interpretation, "the Agency's withholding of the case summaries (as edited to preserve anonymity) cannot be upheld by reliance on the second exemption." *Id.*, at 26.[8]

IV

Additional questions are involved in the determination whether Exemption 6 exempts the case summaries from mandatory disclosure as "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." The first question is whether the clause "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" modifies "personnel and medical files" or only "similar files." The Agency argues that Exemption 6 distinguishes "personnel" from "similar" files, exempting all "personnel files" but only those "similar files" whose disclosure constitutes "a clearly unwarranted invasion of personal privacy," and that the case summaries sought here are "personnel files." On this reading, if it is determined that the case summaries are "personnel files," the Agency argues that judicial inquiry is at an end, and that the Court of Appeals therefore erred in remanding for determination whether disclosure after redaction would constitute "a clearly unwarranted invasion of personal privacy."

The Agency did not argue its suggested distinction between "personnel" and "similar" files to either the District Court or the Court of Appeals, and the opinions of both courts treat Exemption 6 as making no distinction between "personnel" and "similar" files in the application of the "clearly unwarranted invasion of personal privacy" requirement. The District Court held that "[i]t is only the identifying connection to the individual that casts the personnel, medical, and similar files within the protection of [the] sixth exemption." Petition for Certiorari, at 31A. The Court of Appeals stated, "[W]e are dealing here with 'personnel' or 'similar' files. But the key words, of course, are 'a clearly unwarranted invasion of personal privacy' . . . ." 495 F. 2d at 266.

We agree with these views, for we find nothing in the wording of Exemption 6 or its legislative history to support the Agency's claim that Congress created a blanket exemption for personnel files. Judicial interpretation has uniformly reflected the view that no reason would exist for nondisclosure in the absence of a showing of a clearly unwarranted invasion of privacy, whether the documents are filed in "personnel" or "similar" files. See, *e. g.*, *Wine Hobby USA, Inc.* v. *IRS*, 502 F. 2d 133, 135 (CA3 1974); *Rural Housing Alliance* v. *Department of Agriculture*, 162 U.S. App. D.C., 122, 126, 498 F. 2d 73, 77 (1974); *Vaughn* v. *Rosen*, 157 U.S. App. D.C. 340, 484 F. 2d 820 (1973; *Getman* v. *NLRB*, 146 U.S. App. D.C. 209, 213, 450 F. 2d 670, 674 (1971). Congressional concern for the protection of the kind of confidential personal data usually included in a personnel file is abundantly clear. But Congress also made clear that nonconfidential matter was not to be insulated from disclosure merely because it was stored by the Agency in "personnel" files. Rather, Congress sought to construct an exemption that would require a balancing of the individual's right of privacy against the preservation of the basic purpose of the Freedom of Information Act "to open agency action to the light of public scrutiny." The device adopted to achieve that balance was the limited exemption, where privacy was threatened, for "clearly unwarranted" invasions of personal privacy.

Both House and Senate Reports can only be read as disclosing a congressional purpose to eschew a blanket exemption for "personnel . . . and similar files" and to require a balancing of interests in either case. Thus the House Report states, H. R. Rep. No. 1497, at 11, "The limitation of a 'clearly unwarranted invasion of personal privacy' provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to Government informtaion by excluding those kinds of files the disclosure of which might harm the individual." Similarly, the Senate Report, S. Rep. No. 813, at 9, states, "The

[8] The Agency suggests that the disclosure of the identities of disciplined cadets through release of the case summaries will weaken the Honor and Ethics Codes, principally because other cadets will be less likely to report misconduct if they cannot be assured of the absolute confidentiality of their reports. But even assuming that this speculation raises an argument under Exemption 2—rather than Exemption 6 alone—it is unpersuasive in light of the deletion process ordered by the Court of Appeals to be conducted on remand.

phrase 'clearly unwarranted invasion of personal privacy' enunciates a policy that will involve a balancing of interests between the protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information."[9] Plainly Congress did not itself strike the balance as to "personnel files" and confine the Courts to striking the balance only as to "similar files." To the contrary, Congress enunciated a single policy, to be enforced in both cases by the courts, "that will involve a balancing" of the private and public interests." This was the conclusion of the Court of Appeals of the District of Columbia Circuit as to medical files, and that conclusion is equally applicable to personnel files.

"Exemption 6 of the Act covers '. . . medical files . . . the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.' Where a purely medical file is withheld under authority of Exemption 6, it will be for the District Court ultimately to determine any dispute as to whether that exemption was properly invoked." *Ackerly* v. *Ley*, 137 U.S. App. D.C. 133, 136–137 n. 3, 420 F. 2d 1336, 1339–1340 n. 3 (1969) (ellipsis in Court of Appeals opinion). See also *Wine Hobby U.S.A., Inc.* v. *IRS*, 502 F. 2d 133, 135 (CA3 1974).

Congress' recent action in amending the Freedom of Information Act to make explicit its agreement with judicial decisions[11] requiring the disclosure of nonexempt portions of otherwise exempt files is consistent with this conclusion. Thus, § 552(b) now provides that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." Pub. L. 93–502, § 2(c), 88 Stat. 1561, 1564.[12] And § 552(a)(4)(B) was added explicitly to authorize *in camera* inspection of matter claimed to be exempt "to determine whether such records *or any part* thereof shall be withheld." Pub. L. 93–502, § 1(b)(2)(B), 88 Stat., at 1562 (emphasis supplied). The Senate Report accompanying this legislation explains, without distinguishing "personnel and medical files" from "similar files," that its effect is to require courts, "to look beneath the label on a file or record when the withholding of information is challenged. . . . [W]here files are involved [courts will] have to examine the records themselves and require disclosure of portions to which the purposes of the exemption under which they are withheld does not apply." S. Rep. No. 854, 93d Cong., 2d Sess., 32.

The remarks of Senator Kennedy, a principal sponsor of the amendments, make the matter even clearer:

"For example, deletion of names and identifying characteristics of individuals would in some cases serve the underlying purpose of exemption 6, which exempts 'personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.'" 120 Cong. Rec. S. 9315 (daily ed. May 30, 1974).

In so specifying, Congress confirmed what had perhaps been only less clear earlier. For the Senate and House Reports on the Bill enacted in 1966 noted specifically that Health, Education, and Welfare files, Selective Service files, or

---

[9] The Report states further (*ibid.*): "At the same time that a broad philosophy of 'freedom of information' is enacted into law, it is necessary to protect certain equally important rights of privacy with respect to certain information in Government files, such as medical and personnel records. . . .

"It is not an easy task to balance the opposing interests, but it is not an impossible one either. It is not necessary to conclude that to protect one of the interests, the other must, of necessity, either be abrogated or substantially subordinated. Success lies in providing a workable formula which encompasses, balances, and protects all interests, yet places emphasis on the fullest responsible disclosure."

[10] See generally H.R. Rep. No. 1497, at 11: "A *general* exemption for the category of information is much more practical than separate statutes protecting each type of personal record. The limitation of 'a clearly unwarranted invasion of personal privacy' provides a proper balance . . ." (Emphasis supplied.) The Senate Report, as well, speaks of a "general exemption" which is "held within bounds by the use of the limitation of 'a clearly unwarranted invasion of personal privacy.'" S. Rep. No. 813, at 9.

[11] *E. g.*, *Vaughn* v. *Rosen*, 157 U.S. App. D.C. 340, 345, 484 F.2d 820, 825 (1973); *Soucie* v. *David*, 145 U.S. App. D.C. 144, 156, 448 F.2d 1067, 1079 (1971); *Bristol-Myers Co.* v. *FTC*, 138 U.S. App. D.C. 22, 26, 424 F.2d 935, 938–939 (1970). Accord, *Rural Housing Alliance* v. *Department of Agriculture*, 162 U.S. App. D.C. 122, 126–127, 498 F.2d 73, 78 (1974). Cf. § 552(a)(2), providing that

"To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation or staff manual or instruction."

[12] The Senate Report on this amendment cited with evident approval the decision of the Court of Appeals in this case remanding to the District Court for redaction of the case summaries to accommodate the dual interests. S. Rep. No. 854, 93d Cong., 2d sess., 31–32 (1974).

Veterans' Administration files, which as the Agency here recognizes[13] were clearly included within the congressional conception of "personnel files,"[14] were nevertheless intended to be subject to mandatory disclosure in redacted form if privacy could be sufficiently protected. As the House Report states, H.R. Rep. No. 1497, at 11, "The exemption is also intended to cover detailed Government records on an individual which can be identified as applying to that individual and not the facts concerning the award of a pension or benefit or the compilation of unidentified statistical information from personal records." Similarly, the Senate Report emphasized, S. Rep. No. 813, at 9, "For example, health, welfare, and selective service records are highly personal to the person involved yet facts concerning the award of a pension or benefit should be disclosed to the public."

Moreover, even if we were to agree that "personnel files" are wholly exempt from any disclosure under Exemption 6, it is clear that the case summaries sought here lack the attributes of "personnel files" as commonly understood. Two attributes of the case summaries require that they be characterized as "similar files." First, they relate to the discipline of cadet personnel, and while even Air Force Regulations themselves show that this single factor is insufficient to characterize the summaries as "personnel files,"[15] it supports the conclusion that they are "similar." Second, and most significantly, the disclosure of these summaries implicates similar privacy values; for as said by the Court of Appeals, 495 F. 2d, at 267, "identification of disciplined cadets—a possible consequence of even anonymous disclosure—could expose the formerly accused men to lifelong embarrassment, perhaps disgrace, as well as practical disabilities, such as loss of employment or friends." See generally, *e.g.*, *Wine Hobby USA, Inc.* v. *IRS*, 502 F. 2d 133, 135–137 (CA3 1974); *Rural Housing Alliance* v. *Department of Agriculture*, 162 U.S. App. D.C. 122, 125–126, 498 F. 2d 73, 76–77 (1974); *Robles* v. *EPA*, 484 F. 2d 843, 845–846 (CA4 1973). But these summaries, collected only in the Honor and Ethics Code Reading Files and the Academy's Honor Records, do not contain the "vast amounts of personal data," S. Rep. No. 813, at 9, which constitute the kind of profile of an individual ordinarily to be found in his personnel file: showing, for example, where he was born, the names of his parents, where he has lived from time to time, his high school or other school records, results of examinations, evaluations of his work performance. Moreover, access to these files is not drastically limited, as is customarily true of personnel files, only to supervisory personnel directly involved with the individual (apart from the personnel department itself), frequently thus excluding even the individual himself. On the contrary, the case summaries name no names except in guilty cases, are widely disseminated for examination by fellow cadets, contain no facts except such as pertain to the alleged violation of the Honor or Ethics Codes, and are justified by the Academy solely for their value as an educational and instructional tool the better to train military officers for discharge of their important and exacting functions. Documents treated by the Agency in such a manner cannot reasonably be claimed to be within the common and congressional meaning of what constitutes a "personnel file" within Exemption 6.

The Agency argues secondly that, even taking the case summaries as files to which the "clearly unwarranted invasion of personal privacy" qualifications ap-

---

[13] Brief for Petitioners, at 13–16.

[14] There is sparse legislative history as to the precise scope intended for the term "personal files," a detail which itself suggests that Congress intended that particular characterization not to be critical in the application of Exemption 6. But it is quite clear from the Committee Reports that the primary concern of Congress in drafting Exemption 6 was to provide for the confidentiality of personal matters in such files as those maintained by the Department of Health, Education, and Welfare, the Selective Service, and the Veterans' Administration. S. Rep. No. 813, at 9; H.R. Rep. No. 1497, at 11. Moreover, the Senate Report on S. 1666, the principal source for the Bill ultimately enacted as the Freedom of Information Act, and Exemption 6 in particular, specifically refers to such files as "personnel files." S. Rep. No. 1219, 89th Cong., 2d sess., 14. See also Hearings on H.R. 5012 before a Subcommittee of the House Committee on Government Operations, 89th Cong., 1st sess., at 265, 267 (1965) ("Analysis of Agency Comments on S. 1666").

[15] Air Force Regulations in force at the time of the decisions below drew a distinction between "personnel and medical files," 32 CFR § 806.5 (f), and "files similar to medical and personnel files," 32 CFR § 806.5 (g), which clearly categorized case summaries among the latter: "Examples of similar files are those . . . containing reports, records, and other material pertaining to *personnel matters* in which administrative action, including *disciplinary action*, may be taken or has been taken." 32 CFR § 806.5 (g)(1)(ii) (1974); 36 Fed. Reg. 4700, 4701 (1971) (emphasis supplied). After the Court of Appeals' decision, these regulations were amended *inter alia* deleting the last four words, 32 CFR § 806.23 (f)(1)(ii), 40 Fed. Reg. 7901, 7904 (1975), but this alteration is in any event insignificant to the point here.

plies, the Court of Appeals nevertheless improperly ordered the Agency to produce the case summaries in the District Court for an *in camera* examination to eliminate information that could result in identifying cadets involved in Honor or Ethics Code violations. The argument is, in substance, that the recognition by the Court of Appeals of "the harm that might result to the cadets from disclosure" itself demonstrates "[t]he ineffectiveness of excision of names and other identifying facts as a means of maintaining the confidentiality of persons named in government reports . . ." Brief for Petitioners, at 17–18.

This contention has no merit. First, the argument implies that Congress barred disclosure in any case in which the conclusion could not be guaranteed that disclosure would not trigger recollection of identity in any person whatever. But this ignores Congress limitation of the exemption to cases of "clearly unwarranted"[16] invasions of personal privacy.[17] Second, Congress vested the courts with the responsibility ultimately to determine "de novo" any dispute as to whether the exemption was properly invoked in order to constrain agencies from withholding nonexempt matters.[18] No court has yet seen the case histories, and the Court of Appeals was therefore correct in holding that the function of examination must be discharged in the first instance by the District Court. *Ackerly* v. *Ley*, *supra*; *Rural Housing Alliance* v. *Department of Agriculture*, *supra*.

In striking the balance whether to order disclosure of all or part of the case summaries, the District Court, in determining whether disclosure will entail a "clearly unwarranted" invasion of personal privacy, may properly discount its probability in light of Academy tradition to keep identities confidential within the Academy.[19] Respondents sought only such disclosure as was consistent with this tradition. Their request for access to summaries "with personal references or other identifying information deleted," respected the confidentiality interests embodied in Exemption 6. As the Court of Appeals recognized, however, what constitutes identifying information regarding a subject cadet must be weighed not

---

[16] The addition of this qualification was a considered and significant determination. *Robles* v. *EPA*, 484 F.2d 843, 846; (CA4 1973), *Getman* v. *NLRB*, 146 U.S. App. D.C. 209, —, 450 F.2d 670, 674 (1971).The National Labor Relations Board and Treasury Department urged at the hearings on the Act that the "clearly" or "clearly unwarranted" qualification in Exemption 6 be deleted. See Hearings on S. 1160 before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, 89th Cong., 1st sess., 36 (Treasury), 491 (NLRB) (1965); Hearings on H.R. 5012 before a Subcommittee of the House Committee on Government Operations, 89th Cong., 1st sess., 56, 230 (Treasury), 257 (NLRB) (1965). See also Hearings on S. 1160, *supra*, 417 (Department of Defense; objecting to "heavy" burden of showing a *clearly unwarranted* invasion of personal privacy). But see also Hearing on H.R. 5012, *supra*, 151 (testimony of Clark R. Molenhoff, Vice Chairman, Sigma Delta Chi Committee for Advancement of Freedom of Information; advocating the retention of "clearly" in Exemption 6). The terms objected to were nevertheless retained, as a "proper balance," H.R. No. 1497, at 11, to keep the "scope of the exemption . . . within bounds," S. Rep. No. 819, at 9.

The legislative history of the 1974 amendment of Exemption 7, which applies to investigatory files compiled for law enforcement purposes, stands in marked contrast. Under H.R. 12471, 93rd Cong., 2d sess. (1947), as originally amended and passed by the Senate, 120 Cong. Rec. S. 9329, 9337, 9343 (daily ed. May 30, 1974), although not as originally passed by the House, 120 Cong. Rec. H. 1802–1803 (daily ed. Mar. 14, 1974), Exemption 7 was amended to exempt investigatory files compiled for law enforcement purposes only to the extent that their production would "constitute a clearly unwarranted invasion of personal privacy" or meet one of several other conditions. In response to a Presidential request to delete "clearly unwarranted" from the amendment in the interests of personal privacy, the Conference Committee dropped the "clearly," 120 Cong. Rec. S. 17829 (daily ed, Oct. 1, 1974) (letters between President Ford and Senator Kennedy), H. 10002 (daily ed, Oct. 7, 1974) (letters between President Ford and Congressman Moorhead), and the Bill was enacted as reported by the Conference, Public Law 93-502, § 2 (b), 88 Stat. 1561, 1563.

[17] The Court of Appeals held that the argument raised by the Agency that courts have a broad equitable power to decline to order release when disclosure would damage the public interest was not a substantial one in the context of Exemption 6, since that Exemption itself requires a court to exercise a large measure of discretion. 495 F. 2d, at 269. The Agency has not renewed this argument in this Court.

[18] 5 U.S.C. § 552 (a)(4)(B). One of the prime shortcomings of § 3 of the Administrative Procedure Act, in the view of the Congress which passed the Freedom of Information Act, was precisely that it provided no judicial remedy for the unauthorized withholding of agency records. *EPA* v. *Mink*, 410 U.S., at 79.

[19] The legislative history is clear that Exemption 6 was directed at threats to privacy interests more palpable than mere possibilities. The House Report explains that the exemption was intended to exclude files "the disclosure of which might harm the individual . . . [or] detailed Government records on an individual which *can* be identified as applying to that individual. . . ." H.R. Rep. No. 1497, at 11 (emphasis supplied). And the Senate Report states that the balance to be drawn under Exemption 6's "clearly unwarranted invasion of personal privacy" clause is one between "the protection of an individual's private affairs from *unnecessary* public scrutiny, and the preservation of the public's right to governmental information." S. Rep. No. 813, at 9 (emphasis supplied)

only from the viewpoint of the public, but also from the vantage of those who would have been familiar, as fellow cadets or Academy staff, with other aspects of his career at the Academy. Despite the summaries' distribution within the Academy, many of this group with earlier access to summaries may never have identified a particular cadet, or may have wholly forgotten his encounter with Academy discipline. And the risk to the privacy interests of a former cadet, particularly one who has remained in the military, posed by his identification by otherwise unknowing former colleagues or instructors cannot be rejected as trivial. We nevertheless conclude that consideration of the policies underlying the Freedom of Information Act, to open public business to public view when no 'clearly unwarranted" invasion of privacy will result, requires affirmance of the holding of the Court of Appeals, 495 F. 2d, at 267, that although ". . . no one can guarantee that all those who are 'in the know' will hold their tongues, particularly years later when time may have eroded the fabric of cadet loyalty," it sufficed to protect privacy at this stage in these proceedings by enjoining the District Court, *id.*, at 268, that if in its opinion deletion of personal references and other identifying information "is not sufficient to safeguard privacy, then the summaries should not be disclosed to [respondents]." We hold, therefore, in agreement with the Court of Appeals, "that the in camera procedure [ordered] will further the statutory goal of Exemption Six: a workable compromise between individual rights 'and the preservation of public rights to Government information.' " *Id.*, at 269.

To be sure, redaction cannot eliminate all risks of identifiability, as any human approximation risks some degree of imperfection, and the consequences of exposure of identity can admittedly be severe. But redaction is a familiar technique in other contexts[20] and exemptions to disclosure under the Act were intended to be practical workable concepts. *Mink* v. *EPA*, 410 U.S., at 79; S. Rep. No. 813, at 5; H. R. Rep. No. 1497, at 2. Moreover, we repeat, Exemption 6 does not protect against disclosure every incidental invasion of privacy—only such disclosures as constitute "clearly unwarranted" invasions of personal privacy.

Affirmed.

Mr. Justice Stevens took no part in the consideration or decision of this case.

Mr. Chief Justice Burger, *dissenting*

If "hard cases make a bad law," unusual cases surely have the potential to make even worse law. Today, on the basis of a highly unusual request for information about a very unique governmental process, a military academy honor system, the Court interprets definitively a substantial and very significant part of a major federal statute governing the balance between the public's "right-to-know" and the privacy of the individual citizen.

In my view, the Court makes this case carry too much jurisprudential baggage. Consequently, the basic congressional intent to protect a reasonable balance between the availability of information in the custody of the government and the particular individual's right of privacy is undermined. In addition, district courts are burdened with a task Congress could not have intended for them.

(1) This case does not compel us to decide whether the summaries at issue here are "personnel files" or whether files so categorized are beyond the proviso of Exemption (6) that disclosure constitute "a clearly unwarranted invasion of personal privacy." Even assuming, *arguendo*, that the Government must show that the summaries are subject to the foregoing standard, it is quite clear, in my view, that the material at issue here constitutes such an invasion, no matter what excision process is attempted by a federal judge.

The Court correctly notes that Congress, in enacting Exemption 6, intended to strike "a proper balance between the protection of the individual's right of privacy and the preservation of the public's right to Government information by excluding those kinds of files the disclosure of which might harm the individual." H. R. Rep. No. 1497, at 11. Having acknowledged the necessity of such a balance, however, the Court, in my view, blandly ignores and thereby frustrates the congressional intent by refusing to weigh, realistically, the grave consequences implicit in release of this particular information, in any form, against the relatively inconsequential claim of "need" for the material alleged in the complaint.

[20] The Court of Appeals cited as examples Revenue Rulings collected in the Cumulative Bulletin of the Internal Revenue Service, and American Bar Association "Opinions on Professional Ethics" (1967). 45 F.2d at 268 n. 18.

The opinions of this Court have long recognized the opprobrium which both the civilian and the military segments of our society attribute to allegations of dishonor among commissioned officers of our Armed Forces. See, *e.g.*, *Parker* v. *Levy*, 417 U.S. 733, 744 (1974), quoting *Orloff* v. *Willoughby*, 345 U.S. 83, 91 (1953). The stigma which our society imposes on the individual who has accepted such a position of trust [2] and abused it is not erasable, in any realistic sense, by the passage of time or even by subsequent exemplary conduct. The absence of the broken sword, the torn epaulets and the *Rogue's March* from our military ritual does not lessen the indelibility of the stigma. Significantly, cadets and midshipmen—"inchoate officers" [3] have traditionally been held to the same high standards and subjected to the same stigma as commissioned officers when involved in matters with overtones of dishonor.[4] Indeed, the mode of punitive separation as the result of court-martial is the same for both officers and cadets—dismissal. *United States* v. *Ellman*, 9 U.S.C.A.M. 549, 26 C.M.R. 329 (1958). Moreover, as the Court of Appeals noted, it is unrealistic to conclude, in most cases, that a finding of "not guilty" or "discretion" exonerates the cadet in anything other than the purely technical and legal sense of the term.

Admittedly, the Court requires that, before release, these documents be subject to *in camera* inspection with power of excising parts. But, as the Court admits, any such attempt to "sanitize" these summaries would still leave the very distinct possibility that the individual would still be identifiable and thereby injured. In light of Congress' recent manifest concern in the Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1806, 5 U.S.C. § 552a, for "governmental respect for the privacy of citizens . . ." S. Rep. No. 93–1183, 93d Cong. 2d Sess. (1974), it is indeed difficult to attribute to Congress a willingness to subject an individual citizen to the risk of possible severe damage to his reputation simply to permit law students to invade individual privacy to prepare a law journal article. Its definition of a "clearly unwarranted invasion of personal privacy" as equated with "protecting an individual's private affairs from *unnecessary* public scrutiny . . ." S. Rep. No. 813, at 9 (emphasis applied), would otherwise be rendered meaningless.

(2) Moreover, excision would not only be ineffectual in accomplishing the legislative intent of protecting an individual's affairs from unnecessary public scrutiny, but it would place an intolerable burden upon a district court which, in my view, Congress never intended to inflict. Although the 1974 amendments to the Freedom of Information Act require that "[a]ny reasonably segregable portion of a record . . ." 5 U.S.C. § 552 (b), otherwise exempt, be provided, there is nothing in the legislative history of the original Act or its amendments which would require a district court to construct, in effect, a new document. Yet, the excision process mandated here could only require a sweeping reconstruction of the material that the end product would constitute an entirely new document. No provision of the Freedom of Information Act contemplates a federal district judge acting as a "re-write editor" of the original material.

If the Court's holding is indeed a fair reflection of congressional intent, we are confronted with a "split-personality" legislative reaction, by the conflict between a seeming passion for privacy and a comparable passion for needless invasions of privacy.

Accordingly, I would reverse the judgment of the Court of Appeals.

MR. JUSTICE BLACKMUN, DISSENTING

We are here concerned with the Freedom of Information Act, 5 U.S.C. § 552, and with two of the exemptions provided by § 552 (b). The Court in the very recent past, has not hesitated consistently to provide force to the congressionally mandated exemptions. See *FAA Administrator* v. *Robertson*, 422 U.S. 255 (1975); *Renegotiation Board* v. *Grumman Aircraft Engineering Corp.*, 421 U.S. 168

---

[2] As the Court noted in *Orloff* v. *Willoughby*, 345 U.S. 83, 91: "The President's commission . . . recites that 'reposing special trust and confidence in the patriotism, valor, fidelity and abilities of the appointee. . . .'" An officer may be punitively dismissed (the equivalent of a dishonorable discharge) when found guilty of *any* offense by a general court-martial, regardless of the limitations placed on the punishment for the offense when committed by an enlisted personnel. Manual for Courts-Martial, United States 1969 (rev.), ¶ 126d. See generally *United States* v. *Goodwin*, 5 U.S.C.M.A. 647, 18 C.M.R. (1955).

[3] 7 Atty. Gen. 611 (1878).

[4] Article 133, U.C.M.J., 10 U.S.C. § 933 states, for example, "any commissioned officer, *cadet, or midshipman* who is convicted of conduct unbecoming an officer and a gentleman shall be punished as a court-martial may direct." (Emphasis supplied.)

(1975); *NLRB* v. *Sears, Roebuck & Co.*, 421 U.S. 132 (1975); *EPA* v. *Mink*, 410 U.S. 73 (1973). See also *Renegotiation Board* v. *Bannercraft Clothing Co.*, 415 U.S. 1 (1974). Today, I fear, the Court does just the opposite.

A. The Act's second exemption, § 552(b)(2), extends to matters that are "related solely to the internal personnel rules and practices of an agency." There can be no doubt that the Department of the Air Force, including the faculty and staff who supervise cadets at the Air Force Academy, qualifies as an "agency," within the meaning of § 522(b)(2), and the Court so recognizes. *Ante*, at 2. I would have thought, however, that matters that concern the established Honor Codes of our military academies, codes long in existence and part of our military society and tradition, see *Parker* v. *Levy*, 417 U.S. 733, 743, 744 (1974), and the disciplining of cadets as they move along in their Government-supplied education, would clearly qualify as "internal personnel . . . practices" of that agency. By its very nature, this smacks of personnel and personnel problems and practices. It is the agency's internal business and not the public's and, because it is, the exemption is, or should be, afforded. Thus, although the Court does not, I find great support in the language of the second exemption for the petitioners' position here. To me, it makes both obvious and common sense, and I would hold, as did the District Court, that the Act's second exemption applies to the case summaries respondent Rose so ardently desired, and removes them from his eager grasp.

I cannot accept the rationale of the Court of Appeals majority that the existence of a "substantial potential for public interest outside the Government." 495 F. 2d 261, 265 (1974), makes these case summaries any less related "solely" to internal personnel rules and practices. Surely public interest, which is secondary and a by-product, does not measure "sole relationship," which is a primary concept. These summaries involve the discipline, fitness and training of cadets. They are administered and enforced on an academy-limited basis by the cadets themselves, and they exist wholly apart from the formal system of courts-martial and the Uniform Code of Military Justice.

B. The Act's sixth exemption, § 552(b)(6), is equally supportive for the petitioners here and for the result opposite to that the Court reaches today. This exemption applies to matters that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Once again, we have a specific reference to "personnel . . . files," and what I have said above applies equally here. But, in addition, the sixth exemption covers "similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." The added restrictive phrase applies not to "personnel," and surely not to "medical files," but only to "similar files." See *Robles* v. *Environmental Protection Agency*, 484 F. 2d 843, 845–846 (CA4 1973). The emphasis is on personnel files and on medical files and on "similar" files to the extent that privacy invasion of the latter would be unwarranted. The exemption as to personnel files and as to medical files is clear and unembellished. It is almost inconceivable to me that the Court is willing today to attach the qualification phrase to medical files and thereby open to the public what has been recognized as almost the essence of ultimate privacy. The law's long established physician-patient privilege establishes this. Anyone who has had even minimal contact with the practice of medicine surely cannot agree with this extension by judicial construction and with the reasoning of another Court of Appeals in *Ackerly* v. *Ley*, 137 U.S. App. D.C. 133, 136–137, n. 3; 420 F. 2d 1336, 1339–1340, n. 3 (1969), referred to and seemingly approved by the Court. *Ante*, at 19–20.

If, then, these case summaries are something less than "personnel files," a proposition I do not accept, they surely are "similar" to personnel files and, when invaded, afford an instance of a "clearly unwarranted invasion of personal privacy." It is hard to imagine something any more personal. It seems to me that the Court is blinding itself to realities when it concludes, as it does, that Rose's demands do not result in invasions of the personal privacy of the cadets concerned. And I do not regard it as any less unwarranted just because there are court-ordered redaction, a most impractical solution, and judicial rationalization that because the case summaries were posted "on 40 squadron bulletin boards throughout the Academy," *ante*, at 1, and copies distributed to faculty and administration officials, the invasion is not an invasion at all. The "publication" is restricted to the academy grounds and to the private, not public, portions of those facilities. It is disseminated to the corps alone and to faculty and administration, and is a part of the Academy's general pedagogical and

disciplinary purpose and program. To be sure, "40" may appear to some to be a large number, but the Academy's "family" and the area confinement are what are important. And the Court's reasoning must apply, awkwardly it seems to me, to 20 or 10 or five or two posting places, or, indeed, to only one.

I should add that I see little assistance for the Court in the legislative history. As is so often the case, that history cuts both ways and is particularly confusing here. The Court's struggle with it, *ante*, at 9–16, so demonstrates.

Finally, I note the Court's candid recognition of the personnel risks involved. *Ante*, at 27–28. Today's decision, of course, now makes those risks a reality for the cadet, "particularly one who has remained in the military," and the risks are imposed upon the individual in return for a most questionable benefit to the public and personal benefit to respondent Rose. So often the pendulum swings too far.

I fear that the court today strikes a severe blow to the Honor Code, to the system under which they operate, and to the former cadets concerned. It is said to see these old institutions mortally wounded and passing away and individuals placed in jeopardy and embarrassment for lesser incidents long past.

I would reverse the judgment of the Court of Appeals.

MR. JUSTICE REHNQUIST, DISSENTING

Although this case requires our consideration of a claim of a right to "privacy" it arises in quite a different context than some of our other recent decisions such as *Paul* v. *Davis*, —— U. S. ——, decided _____. In that case custodians of public records chose to disseminate them, and one of the subjects of the record claimed that the Fourteenth Amendment to the United States Constitution prohibited the custodian from doing so. Here the custodian of the records, petitioner Department of the Air Force, has chosen *not* to disseminate the records, and his decision to that effect is being challenged by a citizen under the Freedom of Information Act. That Act, as both the Court's opinion and the dissenting opinion of the Chief Justice point out, requires the federal courts to balance the claim of right of access to the information against any consequent "clearly unwarranted invasion of personal privacy." For the reasons stated in Part II of the dissenting opinion of the Chief Justice, I agree that the Act did not contemplate virtual reconstruction of records under the guise of excision of a segregable part of the record. I therefore agree with the Chief Justice and Mr. Justice Blackmun that, in the absence of such redaction, the sixth exemption of the Act is applicable and the judgment of the Court of Appeals should be reversed.

Daniel M. Friedman, Deputy Solicitor General (Robert H. Bork, Solicitor General, Irving Jaffe, Acting Assistant Attorney General, Allan Abbot Tuttle, Assistant to the Solicitor General, Leonard Schaitman and Donald Etra, Justice Dept. attorneys, with him on the brief) for petitioners. Barrington D. Parker, Jr., New York, N.Y. (Melvin L. Wulf and John H. F. Shattuck, with him on the brief) for respondents.

MICHAEL T. ROSE ET AL., PLAINTIFFS-APPELLANTS

v.

DEPARTMENT OF THE AIR FORCE ET AL., DEFENDANTS-APPELLEES

No. 9, Docket 73–1264

UNITED STATES COURT OF APPEALS, SECOND CIRCUIT

ARGUED OCT. 29, 1973—DECIDED MARCH 29, 1974

Action was brought under the Freedom of Information Act to secure disclosure, for purposes of preparation of law review article, of case summaries of Honor and Ethics Code adjudications at service academy. The United States District Court for the Southern District of New York, Lloyd F. MacMahon, J., granted partial summary judgment to defendants, and plaintiffs appealed. The Court of Appeals, Feinberg, Circuit Judge, held that disclosure was not precluded under exemption provision relating to internal personnel rules and practices of an agency; that under exemption applicable where disclosure would constitute a clearly unwarranted invasion of personal privacy, determination of whether the

summaries, with proper names removed, would constitute clearly unwarranted invasion of personal privacy of the affected cadets could not be made without prior inspection by the District Court; and that in light of the large measure of discretion vested in the court under such exemption provision, no further balancing was necessary under any general equity power of the Court to refuse disclosure.

Reversed and remanded with instructions.

MOORE, Circuit Judge, dissented and filed opinion.

1. Records ⇐ 14

The disclosure provisions of the Freedom of Information Act are to be liberally read. 5 U.S.C.A. §§ 552, 552 (a) (3), (c), 1002.

2. Records ⇐ 14

Case summaries of Honor and Ethics Code adjudications at service academy, with identifying information removed, were not exempt from disclosure under section of the Freedom of Information Act exempting matters related solely to the internal personnel rules and practices of an agency, in light of legitimate public interest and future effect on cadets, and in absence of danger to effective operation of the codes at the academy. 5 U.S.C.A. § 552(b) (2).

3. Records ⇐ 14

Guaranteed total success in editing Honor and Ethics Code adjudications at service academy was not required to preclude application of exception in the Freedom of Information Act which applies to matters related solely to the internal personnel rules and practices of an agency. 5 U.S.C.A. § 552 (a) (2), (c).

4. Records ⇐ 14

Each case where disclosure of records under the Freedom of Information Act is resisted under exception applicable where disclosure would constitute a clearly unwarranted invasion of personal privacy involves an essentially unique investigation into the nature of the privacy interest invaded and the extent of the proposed invasion, viewed in light of contemporary mores and sensibilities as applied to the particular facts. 5 U.S.C.A. § 552(b) (6).

5. Records ⇐ 14

For purposes of exception within the Freedom of Information Act applicable where disclosure would constitute a clearly unwarranted invasion of personal privacy, privacy may be as effectively infringed by reviving dormant memories as by imparting new information. 5 U.S.C.A. § 552(b) (6).

6. Records ⇐ 14

In light of fact that disclosure of case summaries from service academy's honor and ethics code adjudications, with identifying information deleted, could expose histories of formerly accused cadets to persons other than military officers and could revive dormant memories and in light of fact that none of the parties to the lawsuit was committed first and foremost to the interests of the effected cadets, agency's internal dissemination of the summaries could not lessen the concerned cadets' right to privacy as embodied in exemption provision of the Freedom of Information Act. 5 U.S.C.A. § 552(b) (6).

7. Records ⇐ 14

In light of possible consequences of even anonymous disclosure, service academy was not obliged under the Freedom of Information Act, without any prior inspection by court, to turn over case summaries of honor and ethics code adjudications with only proper names removed, as such might constitute a clearly unwarranted invasion of personal privacy; but neither could it be determined without such inspection that the exemption covered all or any part of the summaries at issue. 5 U.S.C.A. § 552(b) (6).

8. Records ⇐ 14

Generally, the Freedom of Information Act restrains the use of broad judicial discretion to block disclosure. 5 U.S.C.A. § 552.

9. Records ⇐ 14

In light of large measure of discretion involved in balancing issues necessary to determination of Freedom of Information Act exemption precluding "wholly

unwarranted invasion of personal privacy," no further balancing was required under the notion of general equity power to refuse disclosure, in case involving case summaries of service academy honor and ethics code adjudications. 5 U.S. C.A. §§ 552, 552(b)(6).

Barrington D. Parker, Jr., New York City (American Civil Liberties Union Foundation, John H. F. Shattuck, Melvin L. Wulf, Sanford Jay Rosen, New York City, on the brief), for plaintiffs-appellants.

Leonard Schaitman, Asst. Chief, Appellate Section, Dept. of Justice, Washington, D.C. (Harlington Wood, Jr., Asst. Atty. Gen., Donald Etra, Atty., Dept. of Justice, Whitney North Seymour, Jr., U.S. Atty., S. D. N. Y., William R. Bronner, Gerald A. Rosenberg, T. Gorman Reilly, Asst. U.S. Attys., on the brief), for defendants-appellees.

Before MOORE, HAYS and FEINBERG, Circuit Judges.

FEINBERG, Circuit Judge:

We are faced in this case with construing two of the exemptions in the Freedom of Information Act (the Act), 5 U.S.C. § 552, one of the many recent federal statutes that bring new and difficult cases into the federal courts.[1] As is frequently the case with such legislation, we have little to guide us in the way of precedent, and the brevity and generality of the statutory formulations leave much to be decided by the courts.

I.

Appellant Michael T. Rose, a graduate of the United States Air Force Academy (the Academy) was—at the time this complaint was filed—a third year student at the New York University Law School and a member of the Law Review. Together with other students and members of the Review, Rose has been conducting a survey of disciplinary systems at various Service Academies; the study is slated for publication in a forthcoming issue of the Review.[2] In order to document discussion of the Academy's Honor and Ethics Codes, Rose asked the Academy in autumn 1971 to give him copies of case summaries of Honor and Ethics Code adjudications, which were kept in the Academy's files. The Department of the Air Force refused on the ground that these summaries are exempted from compulsory release by 5 U.S.C. § 552(b)(6), which permits an agency to withhold certain information to avoid unwarranted invasion of privacy.[3]

After exhausting his administrative remedies, Rose joined with appellants Charles P. Diamond and Lawrence B. Pedowitz (who were then, respectively, the current and former Editor-in-Chief of the Review) in this lawsuit under the Act to compel disclosure of the disputed items "with personal references or other identifying information deleted . . .". Judge Lloyd F. MacMahon of the United States District Court for the Southern District of New York granted appellees (collectively the Agency) summary judgment on the issue of the case summaries.[4] Although ultimately ruling against appellants, the judge agreed with them in large part. The Agency put forth two grounds in the district court to support its non-production of the documents: the Act's "personal privacy" exemption, referred to above, and the court's "equitable discretion" to deny disclosure. The judge rejected both arguments. However, he ruled for appellees on a third ground not advanced by them, that the summaries were covered by the exemption in 5 U.S.C. § 552(b)(2) for an agency's internal rules and practices. Attacking the district court's order refusing them access to the summaries, appellants prosecute this appeal. We reverse and remand for further proceedings conforming with this opinion.

---

[1] See Associated Indus. of N.Y.S., Inc. v. United States Dep't of Labor, 487 F. 2d 342, 344–345 and n. 1 (2d Cir. 1973) and statutes cited therein.

[2] Its tentative title is "The Administrative Adjudicatory Systems of the Service Academies: Constitutional Powers and Limitations."

[3] The Air Force also relied on the corresponding Air Force Regulations, A.F.R. 12–30.4f and 12–30.4g(1)(b), 32 C.F.R. § 806.5 (f), (g)(1)(ii) (1972).

[4] The district court granted appellants summary judgment with regard to the third item requested, a complete study of resignations by Academy graduates from the Air Force. Appellees have already complied with this portion of the court's directive, and thus do not appeal from it.

II.

[1] We begin by stressing that the Freedom of Information Act[5] was passed in an effort to cure the defects of former section 3 of the Administrative Procedure Act (APA), 5 U.S.C. § 1002 (1964), which "was generally recognized as falling far short of its disclosure goals and came to be looked upon more as a withholding statute than a disclosure statute."[6] Courts have noted that the Act's remedial purpose was to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny. See e.g., Hawkes v. Internal Revenue Service, 467 F.2d 787, 791 (6th Cir. 1972); Bristol-Myers Co. v. FTC, 138 U.S.App.D.C. 22, 424 F.2d 935, 938, cert. denied, 400 U.S. 824, 91 S.Ct. 46, 27 L.Ed.2d 52 (1970). They have accordingly held that exemptions must be narrowly construed. Vaughn v. Rosen, 484 F.2d 820, 823 (D.C.Cir 1973), cert. denied, 415 U.S. 977, 94 S. Ct. 1564, 39 L.Ed.2d 873 (1974); Soucie v. David, 145 U.S.App.D.C. 144, 448 F. 2d 1067, 1080 (1971). This liberal reading of the Act's disclosure provisions is supported not only by legislative history but, more importantly, by the statutory language, as well. The Act mandates release of documents to "any person"[7] (subject to explicitly defined exemptions)[8] grants to the district courts jurisdiction to enjoin improper withholding after a hearing "de novo" in which "the burden is on the agency to sustain its action," 5 U.S.C. § 552(a)(3); and further calls for disclosure "except as *specifically* stated in this section." 5 U.S.C. § 552(c) (emphasis added).[9] With this background in mind, we turn to a discussion of the applicability of Exemption Two, 5 U.S.C. § 552(b)(2), the provision thought by the district court to support the Agency's refusal to turn over the contested summaries to appellants.

[2] As already indicated, until the district court ruled none of the appellees had thought to rely on Exemption Two in refusing to turn over the case sum-

---

[5] 80 Stat. 250 (1966), codified by 81 Stat. 54 (1967), 5 U.S.C. § 552.

[6] Environmental Protection Agency v. Mink, 410 U.S. 73, 79, 93 S.Ct. 827, 832, 35 L.Ed. 2d 119 (1973). See also S. Rep. No. 813, 89th Cong., 1st Sess. 3, 4–6 (1965) [hereinafter Senate Rep.]; H.R. Rep. No. 1497, 89th Cong., 2d Sess. 4–6 (1966), U.S. Code Cong. & Admin. News 1966 p. 2418 [hereinafter House Rep.]; Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act, quoted in 20 Admin. L. Rev. 263–316, at 267–68 (1968). See generally Note, The Freedom of Information Act: Shredding the Paper Curtain, 47 St. John's L. Rev. 694 (1973) [hereinafter St. John's Note].

[7] Former section 3 of the APA, 5 U.S.C. § 1002 (1964), provided for disclosure only "to persons properly and directly concerned." Davis, The Information Act: A Preliminary Analysis, 34 U. Chi. L. Rev. 761, 765 (1967) [hereinafter Davis].

[8] 5 U.S.C. § 552(b) lists the exemptions from compulsory disclosure. It states:

This section does not apply to matters that are—

(1) specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) investigatory files compiled forl aw enforcement purposes except to the extent available by law to a party other than an agency;

(8) contained in or related to examination, operating, or condition reports prepared by, or on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

[9] 5 U.S.C. § 552(a)(3) reads as follows:

Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, on request for identifiable records made in accordance with published rules stating the time, place, fees to the extent authorized by statute, and procedure to be followed, shall make the records promptly available to any person. On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo and the burden is on the agency to sustain its action. In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member. Except as to causes the court considers of greater importance, proceedings before the district court, as authorized by this paragraph, take precedence on the docket over all other causes and shall be assigned for hearing at the earliest practicable date and expedited in every day.

5 U.S.C. § 552(c) provides:

This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

maries. That section of the Act, see note 8 supra, shields from required disclosure all "matters that are . . . related solely to the internal personnel rules and practices of an agency . . .". In some instances, the scope of the exemption may be open to considerable doubt since the Senate and House Reports diametrically clash.[10] The former cites as examples of excluded material "rules as to personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and the like." Senate Rep. 8. The latter, on the other hand, exempts from disclosure "[o]perating rules, guidelines, and manuals of procedure for Government investigators or examiners" but not "'matters of internal management' such as employee relations and working conditions and routine administrative procedures. . . ." House Rep. 10. 1966 U.S. Code Cong & Admin. News p. 2427. The Senate Report is thought by many to comply with the statutory language better than the House Report, whose thrust is most frequently toward nondisclosure.[11] This court has not yet taken a firm stand on the issue. Cf. Frankel v. SEC, 460 F.2d 813, 816 & n. 5 (2 Cir.), cert. denied, 409 U.S. 889, 93 S.Ct. 125, 34 L.Ed.2d 146 (1972); Polymers, Inc. v. NLRB, 414 F.2d 999, 1006 (2 Cir. 1969), cert. denied, 396 U.S. 1010, 90 S.Ct. 570, 24 L.Ed.2d 502 (1970). We conclude, however, that the difference of approach between the House and Senate Reports would not affect the result here.

If we adopt the Senate construction of Exemption Two, case summaries of Honor and Ethics Code adjudications clearly fall outside its ambit. Such summaries have a substantial potential for public interest outside the Government. Appelants have drawn our attention to various items such as newspaper excerpts, a press conference by an Academy officer and a White House Press Release, which illustrate the extent of general concern with the working of the Cadet Honor Code. As the press conference and the Press Release show, some of the interest has been generated—or at least enhanced—by acts of the Government itself. Of course, even without such official encouragement, there would be interest in the treatment of cadets, whose education is publicly financed and who furnish a good portion of the country's future military leadership. Indeed, all sectors of our society, including the cadets themselves, have a stake in the fairness of any system that leads, in many instances, to the forced resignation of some cadets. The very study involved in this case bears additional witness to the degree of professional and academic interest in the Academy's student-run system of discipline. Moreover, as we later describe in greater detail, see Part III infra, the case summaries themselves have great impact on the lives and careers of subject cadets. Both of these factors—the legitimate public interest and the future effect on cadets—differentiate the summaries from matters of daily routine like working hours, which, in the words of Exemption Two, do relate "*solely* to the internal personnel rules and practices of an agency." (Emphasis added.)

Similarly, even the House Report, which is usually more agency-oriented, does not sanction withholding the summaries. As we have already noted, the House Report in this respect seems to permit greater disclosure of "matters of internal management," except where knowledge of administrative procedures might help outsiders to circumvent regulations or standards.[12] Release of the summaries, which constitute quasi-legal records, poses no such danger to the effective operation of the Codes at the Academy.

[3] Speculating about a different kind of threat to the effectiveness of the Code, the Agency claims that publication of this material might gravely undermine the whole basis of the Honor Code system, whose proceedings are cloaked in confidentiality. The matter of confidentiality is further discussed in Part III infra. It is enough here to point out that appellants have sought only "sanitized" versions of the case summaries with names "or other identifying information" removed. In response to the reaction point, the Agency argues "that there is no

---

[10] See generally Project, Federal Administrative Law Developments—1972, Developments Under the Freedom of Information Act—1972, 1973 Duke L.J. 178, 187–89 [hereinafter Duke Project]; St. John's Note 716–17; Davis 785–86.

[11] Davis 762–63, 785–86; St. John's Note 697. See Hawkes v. Internal Revenue Service, 467 F.2d 787, 794 (6th Cir. 1972), pointing out, inter alia, that the Senate Report furnishes the surer guide to congressional intent since it alone was before both Houses (the Senate passed the bill first); German v. NLRB, 146 U.S. App.D.C. 209, 450 F.2d 670, 673 n. 8 (1971), and cases cited therein.

[12] See, e.g., Tietze v. Richardson, 342 F. Supp. 610 (S.D.Tex. 1972) (Social Security claims processing guidelines); Cuneo v. Laird, 338 F.Supp. 504 (D.C.D.C. 1972) ("playbook" parts of contract audit manual), remanded sub nom. Cuneo v. Schlesinger, 484 F.2d 1086 (D.C. Cir. 1973); Concord v. Ambrose, 333 F.Supp. 958, 960 (N.D.Cal. 1971) (law enforcement agent training manual) (dictum).

way in which the total success of the deletion process can be guaranteed" and that "the functioning of the Honor and Ethics Codes would be seriously impaired even if inadvertent disclosure is a mere possibility."[12] But "total success"—in editing, as in anything else—is an impossible standard and surely not one imposed by a statute based upon a general philosophy of full agency disclosure to the public. Given this policy, as well as the injunction to construe exceptions to the Act strictly, 5 U.S.C. § 552(c), we think it clear that the Agency's withholding of the case summaries (as edited to preserve anonymity) cannot be upheld by reliance on the second exemption.

III.

[4] The Agency also argues that the summaries sought by appellants fall within the purview of Exemption Six of the Act, 5 U.S.C. § 552(b)(6), which covers "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. . . ." As already indicated, Judge MacMahon did not agree with appellees on this point, but they renew their argument in this court. On its face, Exemption Six appears relevant; we are dealing here with "personnel" or "similar files." But the key words, of course, are "a clearly unwarranted invasion of personal privacy," a wholly conclusory phrase, which requires a court to apply the statutory standard without any definite guidelines. Under these circumstances, precedent lends only marginal aid. Each case involves an essentially unique investigation into the nature of the privacy interest invaded and the extent of the proposed invasion, viewed in the light of contemporary mores and sensibilities as applied to the particular facts.

The data pertinent to our inquiry concern the characteristics and use of the Honor and Ethics Code case summaries. These, the Agency tells us, are extracts of the significant facts in each case heard by the Honor Committee and in some important cases heard by the Ethics Committee. (The Ethics program is administered more informally.) As a matter of custom and procedure, information regarding such cases is required to be held in the strictest confidence. The summaries are, however, posted in the forty squadrons and, upon their official release, Honor Representatives are permitted to discuss any feature of the cases with the cadets for their education. The documents are also distributed to Academy personnel who have a "need to know." (In not guilty or so-called "discretion"[14] cases the name of the accused is deleted; in guilty cases it is not.) Therefore, in practice, the curtain of confidentiality appears to shield these records from the glare of external publicity but not from the eyes of present cadets—and future ones, who can read the summaries of past proceedings in the Honor and Ethics Code reading files.

These being the facts, one might ask in what way release of the summaries—with names omitted—could increase the potential for invading the privacy of affected cadets. To be sure, some cases might be recognized by readers of the Law Review article even in the absence of names, by virtue of the circumstances alone. However, it can be argued, only current and former cadets and Academy officials possess the frame of reference which would enable them to reconstruct the incidents described in the summaries, for only they had had access to these records originally. Under these conditions, one might conclude that disclosure of the summaries poses no greater threat to privacy than the Academy itself countenanced through limited distribution and official posting of the items, and that it therefore constitutes no "invasion" at all. This reasoning was substantially the basis of the district court ruling that Exemption Six did not bar disclosure.

[5] This approach, however, ignores certain practical realities. First, a person's privacy may be as effectively infringed by reviving dormant memories as by imparting new information.[15] Cf. Prosser on Torts 827-28 (4th ed. 1971). For example, a senior officer and ex-cadet might, upon reading a summary or a

---

[13] Appellees' brief at 26 and n. 9.

[14] The Honor Reference Handbook of the Air Force Cadet Wing states that, by vote of six out of eight Honor Representatives, a cadet may be found guilty with discretion and returned to the Wing in good standing. A discretion vote indicates a "conviction that the man has learned a lifelong lesson and that he will thereafter uphold the ethical standards of the Wing." Honor Reference Handbook 44 (1970).

[15] But cf. A.F.R. 12-30.g(2)(a), 32 C.F.R. § 806.5(g)(2):

> In determining whether the release of information would result in a clearly unwarranted invasion of privacy, consideration should be given, in cases such as those involving alleged misconduct, to: (1) The amount of time that has passed since the alleged misconduct. . . .

reference to it, realize for the first time that a man under his command had once been the subject of Academy discipline. It would be cold comfort to the junior officer to be told that his chief had always "known" this fact anyway, although he had long forgotten it or had never made the ultimate connection among various bits of knowledge until the article jogged his recollection.

[6] Then, too, publication of even anonymous summaries could expose the histories of formerly accused cadets to persons other than Air Force officers. Despite the continuing injunction of secrecy, no one can guarantee that all those who are "in the know" will hold their tongues, particularly years later when time may have eroded the fabric of cadet loyalty. Finally, we must remember that none of the parties to this lawsuit is committed first and foremost to the interests of affected cadets. It is no slur on appellees to note that they are primarily defending the integrity of their own procedures while appellants, of course, are pressing for disclosure. In these circumstances, we will not hold that the Agency's internal dissemination of the summaries lessens the concerned cadets' right to privacy, as embodied in Exemption Six.

[7] However, while release of even nameless case histories might constitute an "invasion" of protected interests, the inquiry does not end there. The statute requires the Agency to show that the invasion is "unwarranted"—indeed, that it is "clearly" so. The only opinion at all in point, Getman v. NLRB, 146 U.S. App.D.C. 209, 450 F.2d 670 (1971), held that law professors engaged in an NLRB voting study could compel that agency to provide them with names and addresses of eligible employee voters since disclosure would not entail an impermissible intrusion into privacy.[16] But *Getman* was a much stronger case for plaintiffs than ours since release of the desired information would subject the employees named to nothing more than a telephone request to submit to a voluntary interview. 450 F.2d at 674–675. Here, by contrast, identification of disciplined cadets—a possible consequence of even anonymous disclosure—could expose the formerly accused men to lifelong embarrassment, perhaps disgrace, as well as practical disabilities, such as loss of employment or friends. Viewing this potential for serious harm from the perspective of our society's expanding concern for the protection of privacy, cf. Roe v. Wade, 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973), we refuse to hold that appellees must now, without any prior inspection by a court, turn over the summaries to appellants with only the proper names removed. Such a procedure—posing, as it does, grave risks to the reputations of affected cadets—might "constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6).

In order to keep faith with the Act's overall mandate, however, we equally decline to hold at this time that Exemption Six covers all, or any part of, the summaries in issue. Rather, we follow appellants' alternative suggestion and remand with instructions to the district court to conduct an in camera inspection of the Honor and Ethics Code case histories, which it has never examined. Hawkes v. Internal Revenue Service, 467 F.2d 787 (6th Cir. 1972); Soucie v. David, 145 U.S.App.D.C. 144, 448 F.2d 1067 (1971); Bristol-Myers Co. v. FTC, 138 U.S.App. D.C. 22, 424 F.2d 935, cert. denied, 400 U.S. 824, 91 S.Ct. 46, 27 L.Ed.2d 52 (1970). Under 5 U.S.C. § 552(a)(3), see note 9 supra, the "burden" was on the Agency "to sustain its action" in failing to make the case summaries available. Having failed to carry that burden of justification under Exemption Six in the trial court by means of affidavits or testimony, the Agency must now produce the summaries themselves in court. Environmental Protection Agency v. Mink, 410 U.S. 73, 93, 93 S.Ct. 827, 35 L.Ed.2d 119 (1973), and cooperate with the judge in redacting the records so as to delete personal references and all other identifying information. Cf. 5 U.S.C. § 552(a)(2).[17] The practice of furnishing abstracts of cases, while preserving anonymity, is not unknown to the law.[18] We think it highly likely that the combined skills of court and Agency, applied to the sum-

---

[16] See Note, Invasion of Privacy and the Freedom of Information Act: Getman v. NLRB, 40 Geo. Wash. L. Rev. 527 (1972). We have found only three other appellate decisions dealing with Exemption Six, only one of which—Robles v. Environmental Protection Agency, 484 F. 2d 843 (4th Cir. 1973)—reaches the merits of the claim. Cf. Ackerly v. Ley, 137 U.S. App. D.C. 133, 420 F.2d 1336 (1969); Tuchinsky v. Selective Serv. Sys., 418 F.2d 155 (7th Cir. 1969).

[17] This section, which requires, inter alia, publication of final opinions, statements of policy and administrative staff manuals, contemplates agency deletion of identifying details "[t]o the extent required to prevent a clearly unwarranted invasion of personal privacy. . . ."

[18] See, e.g., Revenue Rulings collected in Cum. Bull. of the IRS; ABA, Opinions on Professional Ethics (1967).

maries,[19] will yield edited documents sufficient for the purpose sought and sufficient as well to safeguard affected persons in their legitimate claims of privacy.[20]

We cannot close this section of the opinion without one further comment. We have read out brother Moore's dissent with a sense of wonderment, since it states that we place our "stamp of approval upon" an "egregious invasion of constitutional rights of privacy." We, of course, do no such thing. We have refused to hold, in the second paragraph before this one, that the Agency is required, without any prior inspection by a court, to turn over the summaries to appellants with only the proper names removed. In addition, we have stated immediately above that personal references and all other identifying information should be deleted from the case summaries. If, in the opinion of the district judge, this is not sufficient to safeguard privacy, then the summaries should not be disclosed to appellants. Obviously, the problem would be a simple one if the Freedom of Information Act did not exist or if the only interest to be considered were that of the cadets. But construing Exemption Six is a much more complex process than is indicated by the dissent which fails to refer to the legislative history of the Act, the policy behind it or the cases construing it. In any event, we believe that the in camera procedure required here will further the statutory goal of Exemption Six: a workable compromise between individual rights "and the preservation of public rights to Government information." House Rep. 11, 1966 U.S. Code Cong. & Admin.News p. 2428.[21]

IV.

As a final point, the Agency contends that the courts have a broad equitable power to decline to order release when disclosure would damage the public interest, and urges that we exercise this jurisdiction to withhold the summaries completely. Judge MacMahon rejected this argument, holding that Congress did not leave to the courts a general option of refusing to enforce the Act's requirement of disclosure even though no statutory exemption applies.

[8, 9] Much ink has been spilled on this issue, both by courts and commentators, and we are told that the legislative history is indeterminate[22] and that the appellate decisions are divided.[23] We are not sure how real the conflict is in most instances, since even the courts that are cited as opposing the motion of general equity power to refuse disclosure recognize that a truly exceptional case might require it. Tennessean Newspapers, Inc. v. Federal Housing Administration, 464 F.2d 657, 662 (6th Cir. 1972); Soucie v. David, 145 U.S. App.D.C. 144, 448 F.2d 1067, 1077 (1971). It may be that the true controversy is over the definition of an exceptional case, since we are clear that generally the Act constrains the use of broad judicial discretion to *block* disclosure. Cf. Renegotiation Board v. Bannercraft Clothing Co., 415 U.S. 1, 94 S.Ct. 1028, 39 L.Ed.2d 123 (1974) (dictum—broad equitable power to enforce the Act). In any event, in the context of Exemption Six the issue is not a substantial one, since the language of the exemption requires a court to exercise a large measure of discretion. This was pointed out by the Court of Appeals for the District of Columbia Circuit, a court

---

[19] It was estimated at oral argument that there were 100–200 summaries.

[20] Cf. House Rep. 11, 1966 U.S. Code Cong. & Admin. News, p. 2448:

The exemption [six] is . . . intended to cover detailed Government records on an individual which can be identified as applying to that individual and not the facts concerning the award of a pension or benefit or the compilation of *unidentified statistical information from personal records.* [Emphasis added.]

[21] Moreover, despite the dissent's gloomy prediction, we do not envision a need for dozens of hours of hard labor by judicial and military officers. On the contrary, once agreement is reached on general principles of redaction the actual process of editing the summaries should not take undue amounts of time.

[22] Compare House Rep. 9 with Senate Rep. 3.

[23] Thus, Duke Project 178–79 n. 9 states that the Fourth, Sixth and D.C. Circuits reject the idea of a general equitable jurisdiction and the Fifth and Ninth Circuits support it. Compare Robles v. Environmental Protection Agency, 484 F. 2d 843, 847 (4th Cir. 1973); Tennessean Newspapers, Inc. v. Federal Housing Administration, 464 F. 2d 657, 661–662 (6th Cir. 1972); Hawkes v. Internal Revenue Service, 467 F. 2d 787, 792 n. 6 (6th Cir. 1972); Wellford v. Hardin, 444 F. 2d 21, 24–25 (4th Cir. 1971); Getman v. NLRB, 146 U.S. App. D.C. 209, 450 F. 2d 670, 677–680 (1971); Soucie v. David, 145 U.S. App. D.C. 144, 448 F. 2d 1067, 1076–1077 (1971), with Wu v. National Endowment for Humanities, 460 F. 2d 1030, 1034 (5th Cir. 1972), cert. denied, 410 U.S. 926, 93 S. Ct. 1352, 35 L. Ed. 2d 586 (1973); Benson v. General Serv. Administration, 415 F. 2d 878 (9th Cir. 1969). But cf. Epstein v. Resor, 421 F. 2d 930, 933 (9th Cir.), cert. denied, 398 U.S. 965, 90 S. Ct. 2176, 26 L. Ed. 2d 549 (1970) (limited role of courts under the first and third exemptions). Prof. Davis also believes in the existence of equitable power to refuse disclosure. Davis 767.

frequently cited for the view that the federal courts have no general equitable jurisdiction to refuse disclosure when on exemption applies: "Any discretionary balancing of competing interests will necessarily be inconsistent with the purpose of the Act to give agencies, and courts as well, definitive guidelines in setting information policies. . . . But Exemption (6), by its explicit language, calls for such balancing and must therefore be viewed as an exception to the general thrust of the Act. S.Rep., at 9, explains:

"The phrase 'clearly unwarranted invasion of personal privacy' enunciates a policy that will involve a balancing of interests between the protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information. The application of this policy should lend itself particularly to those Government agencies where persons are required to submit vast amounts of personal data usually for limited purposes. * * *"

We note in passing that no other exemption specifically requires balancing. In view of the Act's basic purpose to limit discretion and encourage disclosure, we believe that Exemption (6) should be treated as unique, and that equitable discretion should not be imported into any of the other exemptons. . . .

Getman v. NLRB, 146 U.S. App. D.C. 209, 450 F.2d 670, 674 n. 10 (1971).

We have already decided that disclosure of the case summaries would not be "a clearly unwarranted invasion of personal privacy" under Exemption Six, if the summaries are redacted as set forth above. We agree with the court in *Getman* that no further balancing is necessary.[24]

Accordingly, we reverse and remand for further proceedings, consistent with this opinion and expedited pursuant to the command of 5 U.S.C. § 552(a)(3).

MOORE, Circuit Judge (dissenting):

I must express a most vigorous dissent to the majority's judicial stamp of approval upon the egregious invasion of constitutional rights of privacy which their opinion authorizes. At a time when the courts are more and more being called upon to protect an individual's character from being unnecessarily besmirched, when much is being said and written about prison rehabilitation, I am amazed that any court should countenance—much less authorize—the curiosity satisfying efforts of three law school students who, merely to write a Law Review note, would pry into and seek to disclose the former transgressions of Air Force cadets. This is not a case in which the courts can attempt to justify their interposition on the theory that Congress has failed to act and that, therefore, the courts must legislate. Here there is a definite statute of prohibition which the majority now overrides.

When an Air Force cadet is accused of lying, stealing or cheating at the Academy, he is protected by the greatest possible confidentiality. This may arise in part from the fact that this charge has been made possible by the principle of toleration which in grammar schoolyard parlance means "tattletale" or as phrased in the record as "The backbone of the Honor Code is the toleration clause which requires that every cadet report any suspected violation of the Code" (App. 120). Thus, not only must the cadet be protected but also the non-tolerator (tattler).

The hearings, as would be expected, are as sacrosanct as are (or should be) jury room proceedings, namely, "all matters discussed at the hearing are confidential and should not be discussed outside the room with anyone other than an Honor Representative" (App. 164–65). The summaries of each case are kept confidentially restricted except in a small area.

In passing the Freedom of Information Act, 5 U.S.C. § 552, Congress carefully and specifically excluded from public gaze:

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. . . .

If doctor-patient files are protected, how much the more should files dealing with quasi-criminal or possible character-besmirching facts to be kept secret. The disclosure of disease, be it venereal or mental, can be remedied or cured. The drawing of a bar sinister across the escutcheon of a young man entering upon his life's career, cannot be erased.

---

[24] While this case was under advisement, we asked the parties to brief the question of mootness, in view of the possibility that publication of plaintiffs' article would moot the issue. In their response, both sides affirmed their belief that the matter of disclosure of the case summaries was still properly before us. We agreed with this conclusion and therefor proceeded to consider the case on the merits.

The Air Force officials, mindful of their duty to protect their cadets, responded in a manner which should have received the highest judicial commendation instead of disapproval. The Academy's Honor and Ethics Executive, in rejecting plaintiffs' request for the case summaries, stated:

I regret that Academy policy requires denial of public access to honor case files, including selected ones in the Honor Code Reading Files. All of these cases are documented as 'For Official Use Only' and are disseminated for internal use only to the Honor Representatives and those few staff personnel who have a continuing need to understand the workings of the Cadet Honor Code. It would be in poor faith with all cadets who have met honor hearings to allow their cases to come into the public eye. To permit the use of honor cases for such purpose would tend to set a precedent that may operate to the detriment of innocent persons.

"To be accused or found guilty of an honor violation is an emotionally trying experience that should, in due respect for the rights of the individual concerned, be limited as possible. Society in general does not understand the difference in the lying, cheating and stealing that constitutes a Cadet Honor violation as opposed to the degree of criminality required in society at large to cause an equally serious type of censor [sic: censure]. The problems of such misunderstanding and the unnecessary embarrassment that could result seems to exceed the value to be gained from making the case files available to the public."

In denying the request, the Commandant of Cadets stated (App. 30):

"The Air Force Academy will be unable to provide you sample ethics cases. The sample ethics cases used in the Honor Code Reading File are designated 'For Official Use Only'. It is intended that these cases will be used for the edification of the Cadet Wing and Academy staff only. Indiscriminate release of this information to persons without a need to know could be counter to the best interest of the individuals concerned and the Air Force Academy."

When the request reached the Office of the Secretary of the Air Force, the futility of any attempted deletion was pointed out in the statement (App. 35):

"A release of the honor hearing cases and ethics cases would constitute an unwarranted invasion into the privacy of former cadets of the Academy. Some cases may be recognized by the reader by the circumstances alone without the identity of the cadet given. This being the case then the reader could easily connect the incident with the particular cadet involved. Additionally, they are internal documents which are not meant for mass circulation. They are stamped 'For Official Use Only' and are afforded subscribed routing and handling procedures."

The reasons for confidentiality and non-disclosure cannot be better summarized than by the Commandant's Executive for Honor and Ethics, who stated:

"There is no way of determining just how these facts will or could be used. This data could find its way to the relatives, friends and classmate of cadets and supply the missing link in disclosing the identity of a guilty cadet. No person who has made a mistake and been punished should have to have this mistake follow him for the rest of his life."

And, indeed, merely to satisfy the desire of plaintiffs to write a Law Review note, no court should aid and abet a project which could result in having a cadet's "mistake follow him for the rest of his life." (App. 211a).

Deletion of names suggested by the majority would be of no avail. In addition to names, identifiable facts would have to be eliminated. Eliminating all determinative essentials would only create a hypothetical situation.

As the Commandant of Cadets so logically explained:

"The use of these case files or writeups, even if the identity of the individual were not given, could still be an invasion of privacy as the incident may have been so notorious that the reader would immediately recognize the cadet who was the subject of the Honor or Ethics Hearing. In certain instances, the Cadet Wing has given the Honor Committee the prerogative to grant discretion to a cadet who has been voted guilty and to allow him to return to the Cadet Wing. The man who has learned his lifelong lesson of honor can be a great asset to the Wing and to the Air Force. His retention is therefore not only justified; it is desired. . . . Therefore, every effort is made to avoid disclosure of the cadet's name so that he may return to the Wing unblemished to continue his education."

The majority recognize that their decision even with anonymous disclosure "could expose the formerly accused men to lifelong embarrassment, perhaps disgrace, as well as practical disabilities, such as loss of employment or friends." These accused cadets are the real parties in interest; yet, as the majority concedes, "none of the parties to this lawsuit is committed first and foremost to

the interests of affected cadets." Even the unborn child is in many situations entitled to his (or her) guardian *ad litem* and *Gideon*[1] was deemed to be entitled to be heard through counsel. But accused cadets are to be subjected to possible lifelong disgrace or loss of employment without any spokesman.

Of course, Congress never intended any such result. Nor does the Act so decree. Lest any implication to this effect might be gleaned therefrom, Congress wrote therein a specific prohibition against an "unwarranted invasion of personal privacy."

Consider briefly the majority's suggested protection against "this potential for serious harm". First, the Air Force must remove from all case summaries, estimated in open court as involving one hundred to two hundred summaries, all proper names. Then these nameless but not factless summaries are to be turned over to the District Court. There the majority are sure that "the combined skills of court and Agency, * * * will yield edited documents * * * sufficient * * * to safeguard affected persons in their legitimate claims of privacy." But for what purpose and at what cost? The purpose is clear, i.e., to have the Air Force and the District Court co-author a student contribution to a legal periodical. Time cost is another matter. Assuming only one hundred and fifty summaries, vital name excision should be capable of accomplishment in ten minutes per summary—an inconsequential twenty-five hours. However, careful Court editing to eliminate identifying facts would be much more time-consuming. Seventy-five hours of Court time would be conservative. In these days when there is so much clamor about the desirability of speedy trials, I am unwilling to subscribe to, or acquiesce in, any opinion which saddles such a needless burden upon an important branch of our military forces and, in my opinion, an equally important judicial branch. Hence, I dissent.

[From the United States Law Week, 44 LW 4528, Apr. 20, 1976]

UNITED STATES, PETITIONER *v.* MITCHELL MILLER

No. 74–1179

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH DISTRICT

[April 21, 1976]

SYLLABUS

Respondent, who had been charged with various federal offenses, made a pretrial motion to suppress microfilms of checks, deposit slips, and other records relating to his accounts at two banks, which maintained the records pursuant to the Bank Secrecy Act of 1970 (Act). He contended that the subpoenas *duces tecum* pursuant to which the material had been produced by the banks were defective and that the records had thus been illegally seized in violation of the Fourth Amendment. Following the denial of his motion, respondent was tried and convicted. The Court of Appeals reversed, having concluded that the subpoenaed documents fell within a constitutionally protected zone of privacy. *Held:* Respondent possessed no Fourth Amendment interest in the bank records that could be vindicated by a challenge to the subpoenas, and the District Court therefore did not err in not granting the motion to suppress.

(a) The subpoenaed materials were business records of the banks, not respondent's private papers.

(b) There is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities. The Act's record-keeping requirements do not alter these considerations so as to create a pro-

[1] Gideon v. Wainwright, 372 U.S. 325, 83 S. Ct. 792, 9 L. Ed. 2d 799 (1933).

tectable Fourth Aemndment interest of a bank depositor in the bank's records of this account.

(c) Issuance of a subpoena to a third party does not violate a defendant's rights, even if a criminal prosecution is contemplated at the time the subpoena is issued. *California Bankers Assn.* v. *Shultz*, 416 U. S. 21, 53.

(d) Access to bank records under the Act is to be controlled by "existing legal process." That does not mean that greater judicial scrutiny, equivalent to that required for a search warrant, is necessary when a subpoena is used to obtain a depositor's bank records.

500 F. 2d 751, reversed and remanded.

Powell, J., delivered the opinion of the Court, in which Burger C. J., and Stewart, White, Blackmun, Rehnquist, and Stevens, JJ., joined. Brennan and Marshall JJ., filed dissenting opinions.

Mr. Justice Powell delivered the opinion of the Court.

Respondent was convicted of possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax, possessing 175 gallons of whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues. 26 U. S. C. § 5179, 5205, 5601 *et seq.*, 18 U. S. C. § 371. Prior to trial respondent moved to suppress copies of checks and other bank records obtained by means of allegedly defective subpoenas *duces tecum* served upon two banks at which he had accounts. The records had been maintained by the banks in compliance with the requirements of the Bank Secrecy Act of 1970, 12 U. S. C. § 1829b (d).

The District Court overruled respondent's motion to suppress and the evidence was admitted. The Court of Appeals for the Fifth Circuit reversed on the ground that a depositor's Fourth Amendment rights are violated when bank records maintained pursuant to the Bank Secrecy Act are obtained by means of a defective subpoena. It held that any evidence so obtained must be suppressed. Since we find that respondent had no protectable Fourth Amendment interest in the subpoenaed documents, we reverse the decision below.

I

On December 18, 1972, in response to an informant's tip, a deputy sheriff from Houston County, Ga., stopped a van-type truck occupied by two of respondent's alleged co-conspirators. The truck contained distillery apparatus and raw material. On January 9, 1973, a fire broke out in a Kathleen, Ga., warehouse rented to respondent. During the blaze firemen and sheriff department officials discovered a 7,500 gallon-capacity distillery, 175 gallons of nontax-paid whiskey, and related paraphernalia.

Two weeks later agents from the Treasury Department's Alcohol, Tobacco & Firearms Unit presented grand jury subpoenas issued is blank by the clerk of the District court, and completed by the United States Attorney's office, to the presidents of the Citizens & Southern National Bank of Warner Robins and the Bank of Byron, where respondent maintained accounts. The subpoenas required the two presidents to appear on January 24, 1973, and to produce:

"All records of accounts, *i.e.*, savings, checking, loan or otherwise, in the name of Mr. Mitch Miller [respondent], 3859 Mathis Street, Macon, Ga. and/or Mitch Miller Associates, 100 Executive Terrace, Warner Robins, Ga., from October 1, 1972, through the present date [January 22, 1973, in the case of the Bank of Byron, and January 23, 1973, in the case of the Citizens & Southern National Bank of Warner Robins]."

The banks did not advise respondent that the subpoenas had been served but ordered their employees to make the records available and to provide copies of any documents the agents desired. At the Bank of Byron, an agent was shown microfilm records of the relevant account and provided with copies of one deposit slip and one or two checks. At the Citizens & Southern National Bank microfilm records also were shown to the agent, and he was given copies of the records of respondent's account during the applicable period. These included all checks, deposit slips, two financial statements and three monthly statements. The bank presidents were then told that it would not be necessary to appear in person before the grand jury.

The grand jury met on February 12, 1973, 19 days after the return date on the subpoenas. Respondent and four others were indicted. The overt acts alleged to have been committed in furtherance of the conspiracy included there financial transactions—the rental by respondent of the van-type truck, the purchase by

respondent of radio equipment, and the purchase by respondent of a quantity of sheet metal and metal pipe. The record does not indicate whether any of the bank records were in fact presented to the garnd jury. They were used in the investigation and provided "one or two" investigatory leads. Copies of the checks also were introduced at trial to establish the overt acts described above.

In his motion to suppress, denied by the District Court, respondent contended that the bank documents were illegally seized. It was urged that the subpoenas were defective because they were issued by the U.S. Attorney rather than a court, no return was made to a court, and the subpoenas were returnable on a date when the grand jury was not in session. The Court of Appeals reversed. 500 F. 2d 751 (1974). Citing the prohibition in *Boyd* v. *United States*, 116 U.S. 616, 622 (1886), against "compulsory production of a man's private papers to establish a criminal charge against him," the court held that the government had improperly circumvented *Boyd's* protections of respondent's Fourth Amendment right against "unreasonable searches and seizures" by "first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies." 500 F. 2d at 757. The court acknowledged that the recordkeeping requirements of the Bank Secrecy Act had been held to be constitutional on their face in *California Bankers Assn.* v. *Shultz*, 416 U.S. 21 (1974), but noted that access to the records was to be controlled by "existing legal process." See *id.*, at 52. The subpoenas issued here were found not to constitute adequate "legal process." The fact that the bank officers cooperated voluntarily was found to be irrelevant, for "he whose rights are threatened by the improper disclosure here was a bank depositor, not a bank official." 500 F. 2d, at 758.

The Government contends that the Court of Appeals erred in three respects: (i) in finding that respondent had the Fourth Amendment interest necessary to entitle him to challenge the validity of the subpoenas *duces tecum* through his motion to suppress; (ii) in holding that the subpoenas were defective; and (iii) in determining that suppression of the evidence obtained was the appropriate remedy if a constitutional violation did take place.

We find that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress. Because we reverse the decision of the Court of Appeals on that ground alone, we do not reach the Government's latter two contentions.

II

In *Hoffa* v. *United States*, 385 U.S. 293, 301–302 (1966), the Court said that "no interest legitimately protected by the Fourth Amendment" is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into "the security a man relies upon when he places himself or his property within a constitutionally protected area." The Court of Appeals, as noted above, assumed that respondent had the necessary Fourth Amendment interest, pointing to the language in *Boyd* v. *United States*, 116 U.S., at 622, which describes that Amendment's protection against the "compulsory production of a man's private papers."[1] We think that the Court of Appeals erred in finding the subpoenaed documents to fall within a protected zone of privacy.

On their face, the documents subpoenaed here are not respondent's "private papers." Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks. As we said in *California Bankers Assn.* v. *Shultz*, 416 U.S., at 48–49, "[b]anks are . . . not . . . neutrals in transactions involving negotiable instruments, but parties to the istruments with a substantial stake in their continued availability and acceptance" The records of respondent's accounts, like "all of the records [which are required to be kept pursuant to the Bank Secrecy Act,] pertain to transactions to which the bank was itself a party." *Id.*, at 52.

Respondent argues, however, that the Bank Secrecy Act introduces a factor that makes the subpoena in this case the functional equivalent of a search and seizure of the depositor's "private papers." We have held, in *California Bankers*

[1] The Fourth Amendment implications of *Boyd* as it applies to subpoenas *duces tecum* have been undercut by more recent cases. *Fisher* v. *United States*, — U.S. —(1976), slip op., at 15–17. See *infra*, at 10.

Assn. v. *Shultz*, *supra*, at 54, that the mere maintenance of records pursuant to the requirements of the Act "invade[s] no Fourth Amendment right of any depositor." But respondent contends that the combination of the recordkeeping requirements of the Act and the issuance of a subpoena [2] to obtain those records permits the Government to circumvent the requirements of the Fourth Amendment by allowing it to obtain a depositor's private records without complying with the legal requirements that would be applicable had it proceeded against him directly.[3] Therefore, we must address the question whether the compulsion embodied in the Bank Secrecy Act as exercised in this case creates a Fourth Amendment interest in the depositor where none existed before. This question was expressly reserved in *California Bankers Assn.*, *supra*, at 53–54 & n. 24.

Respondent urges that he has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy. He relies on this Court's statement in *Katz* v. *United States*, 389 U.S. 347, 353 (1967), quoting *Warden* v. *Hayden*, 387 U.S. 294, 304 (1967), that "we have . . . departed from the narrow view" that "'property interests control the right of the Government to search and seize,'" and that a "search and seizure" become unreasonable when the Government's activities violate "the privacy upon which [a person] justifiably relie[s]." But in *Katz* the Court also stressed that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." *Id.*, at 351. We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate "expectation of privacy" concerning their contents. Cf. *Couch* v. *United States*, 409 U.S. 322, 335 (1973).

Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings." 12 U.S.C. § 1829b(a)(1). Cf. *Couch* v. *United States*, *supra*, at 335.

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government. *United States* v. *White*, 401 U.S. 745, 751–752 (1971). This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. *Id.*, at 752; *Hoffa* v. *United States*, 385 U.S., at 302; *Lopez* v. *United States*, 373 U.S. 427 (1963).[4]

This analysis is not changed by the mandate of the Bank Secrecy Act that records of depositors' transactions be maintained by banks. In *California Bankers Assn.* v. *Shultz*, *supra*, at 52–53, we rejected the contention that banks, when keeping records of their depositors' transactions pursuant to the Act, are acting solely as agents of the government. But, even if the banks could be said to have been acting solely as government agents in transcribing the necessary information

---

[2] Respondent appears to contend that a depositor's Fourth Amendment interest comes into play only when a *defective* subpoena is used to obtain records kept pursuant to the Act. We see no reason why the existence of a Fourth Amendment interest turns on whether the subpoena is defective. Therefore, we do not limit our consideration to the situation in which there is an alleged defect in the subpoena served on the bank.

[3] It is not clear whether respondent refers to attempts to obtain private documents through a subpoena issued directly to the depositor or through a search pursuant to a warrant. The question whether personal business records may be seized pursuant to a valid warrant is before the Court in No. 74–1646, *Andresen* v. *Maryland*.

[4] We do not address here the question of evidentiary privileges, such as that protecting communications between an attorney and his client. Cf. *Fisher* v. *United States*, — U.S. — (1976), slip op., at 11–12.

and complying without protest[5] with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights. See *Osborn* v. *United States*, 385 U.S. 323 (1966); *Lewis* v. *United States*, 385 U.S. 206 (1966).

III

Since no Fourth Amendment interests of the depositor are implicated here, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena is issued. *California Bankers Assn.* v. *Shultz*, 416 U.S., at 53; *Donaldson* v. *United States*, 400 U.S. 517, 537 (1971) (Douglas, J., concurring). Under these principles, it was firmly settled, before the passage of the Bank Secrecy Act, that an Internal Revenue Service summons directed to a third-party bank does not violate the Fourth Amendment rights of a depositor under investigation. See *First National Bank* v. *United States*, 267 U.S. 576 (1925), aff'g 295 F. 142 (SD Ala. 1924). See also *California Bankers Assn.* v. *Shultz*, *supra*, at 53; *Donaldson* v. *United States*, 400 U.S., at 522.

Many banks traditionally kept permanent records of their depositors' accounts, although not all banks did so and the practice was declining in recent years. By requiring that such records be kept by all banks, the Bank Secrecy Act is not a novel means designed to circumvent established Fourth Amendment rights. It is merely an attempt to facilitate the use of a proper and longstanding law enforcement technique by insuring that records are available when they are needed.[6]

We hold that the District Court correctly denied respondent's motion to suppress, since he possessed no Fourth Amendment interest that could be vindicated by a challenge to the subpoenas.

IV

Respondent contends not only that the subpoenas *duces tecum* directed against the banks infringed his Fourth Amendment rights, but that a subpoena issued to a bank to obtain records maintained pursuant to the Act is subject to more stringent Fourth Amendment requirements than is the ordinary subpoena. In making this assertion he relies on our statement in *California Bankers Assn.*, *supra*, at 52, that access to the records maintained by banks under the Act is to be controlled by "existing legal process."[7]

In *Oklahoma Press Publishing Co.* v. *Walling*, 327 U.S. 186, 208 (1946), the Court said that "the Fourth [Amendment], if applicable [to subpoenas for the production of business records and papers], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." See also *United States* v. *Dionisio*, 410 U.S. 1, 11–12 (1973). Respondent, citing *United States* v. *United States District Court*, 407 U.S. 297 (1972), in which we discussed the application of the warrant requirements of the Fourth Amendment to domestic security surveillance through electronic eavesdropping, suggests that greater judicial scrutiny, equivalent to that required for a search warrant, is necessary when a subpoena is to be used to obtain bank records of a depositor's

---

[5] Nor did the banks notify respondent, a neglect without legal consequences here, however unattractive it may be.

[6] Petitioner does not contend that the subpoenas infringed upon his First Amendment rights. There was no blanket reporting requirement of the sort we addressed in *Buckley* v. *Valeo*, — U.S. — (1976), slip op., at 54–76, nor any allegation of an improper inquiry into protected associational activities of the sort presented in *Eastland* v. *United States Servicemen's Fund*, 421 U.S. 491 (1975).

We are not confronted with a situation in which the Government, through "unreviewed executive discretion," has made a wide-ranging inquiry that unnecessarily "touch[es] upon intimate areas of an individual's personal affairs." *California Bankers Assn.* v. *Shultz*, *supra*, at 78–79 (POWELL, J., concurring). Here the Government has exercised its powers through narrowly directed subpoenas *duces tecum* subject to the legal restraints to such process. See Part IV, *infra*.

[7] This case differs from *Burrows* v. *Superior Court*, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974), relied on by Mr. Justice Brennan in dissent, in that the bank records of respondent's accounts were furnished in response to "compulsion by legal process" in the form of subpoenas *duces tecum*. The court in *Burrows* found it "significant . . . that the bank [in that case] provided the statements to the police in response to an informal oral request for information," 13 Cal. 3d, at 243, 529 P.2d, at 593, 118 Cal. Rptr., at 169.

account. But in *California Bankers Assn., supra,* at 52, we emphasized only that access to the records was to be in accordance with "existing legal process." There was no indication that a new rule was to be devised, or that the traditional distinction between a search warrant and a subpoena would not be recognized.[8]

In any event, for the reasons stated above, we hold that respondent lacks the requisite Fourth Amendment interest to challenge the validity of the subpoenas.[9]

V

The judgment of the Court of Appeals is reversed. The court deferred decision on whether the trial court had improperly overruled respondent's motion to suppress distillery apparatus and raw material seized from a rented truck. We remand for disposition of that issue.

So ordered.

MR. JUSTICE BRENNAN, DISSENTING

The pertinent phrasing of the Fourth Amendment—"The right of the people to be secure in their persons houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"—is virtually *in haec verba* with Art. I, § 13, of the California Constitution—"The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated." The California Supreme Court has reached a conclusion under Art. I, § 13, in the same factual situation, contrary to that reached by the Court today under the Fourth Amendment.[10] I dissent because in my view the California Supreme Court correctly interpreted the relevant constitutional language.

In *Burrows* v. *Superior Court*, 13 Cal. 3d 238, 529 P. 2d 590, 118 Cal. Rptr. 166 (1974), the question was whether bank statements or copies thereof relating to an accused's bank accounts obtained by the sheriff and prosecutor without benefit of legal process,[11] but with the consent of the bank, were acquired as a result of an illegal search and seizure. The California Supreme Court held that the accused had a reasonable expectation of privacy in his bank statements and records, that the voluntary relinquishment of such records by the bank at the request of the sheriff and prosecutor did not constitute a valid consent by the accused, and that the acquisition by the officers of the records therefore was the result of an illegal search and siezure. In my view the same conclusion, for the reasons stated by the California Supreme Court, is compelled in this case under the practically identical phrasing of the Fourth Amendment. Addressing the threshold question whether the accused's right of privacy was invaded, and relying in part on the decision of the Court of Appeals in this case, Mr. Justice Mosk stated in his excellent opinion for a unanimous court.

"It cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business opera-

---

[8] A subpoena *duces tecum* issued to obtain records is subject to no more stringent Fourth Amendment requirements than is the ordinary subpoena. A search warrant, in contrast, is issuable only pursuant to prior judicial approval and authorizes government officers to seize evidence without requiring enforcement through the courts. See *United States* v. *Dionisio, supra,* at 9–10.

[9] There is no occasion for us to address whether the subpoenas complied with the requirements outlined in *Walling*. The banks upon which they were served did not contest their validity.

[10] The expectation of privacy relied upon by respondent to support his Fourth Amendment claim is similar to that rejected as to similar documents in *Couch* v. *United States*, 409 U.S. 322 (1973). But in *Couch* the taxpayer had delivered the documents to her accountant for preparation of income tax returns "knowing that mandatory disclosure of much of the information therein is required in an income tax return." *Id.*, at 335; see *id.*, at 337 (BRENNAN, J., concurring). In contrast, in the instant case the banks were obliged only to respond to lawful process, *California Bankers Assn.* v. *Schultz*, 416 U.S. 21, 52–54 (1974), and had no obligation to disclose the information voluntarily. The expectation of privacy asserted in *Fisher* v. *United States*, — U.S. — (1976), is distinguishable on similar grounds.

[11] The Court distinguishes *Burrows* on the ground that it involved no legal process, while the instant case involves legal process in the form of subpoenas *duces tecum*. *Ante*, at 10 n. 7. But the Court also states that the Fourth Amendment issue does not turn on whether the subpoenas were defective. *Ante*, at 6 n. 2.

In any event, for present purposes I would accept the Court of Appeals' conclusion that the subpoenas in this case were defective. Moreover, although not relied upon by the Court of Appeals, neither the bank nor the Government notified respondent of the disclosure of his records to the Government. In my view, the absence of such notice is not just "unattractive," *ante*, at 8 n. 5, a fatal constitutional defect inheres in a process that omits provision for notice to the bank customer of an invasion of his protected Fourth Amendment interest.

tions, will remain private, and that such an expectation is reasonable. The prosecution concedes as much, although it asserts that this expectation is not constitutionally cognizable. Representatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential.

"In the present case, although the record establishes that copies of petitioner's bank statements rather than his checks were provided to the officer, the distinction is not significant with relation to petitioner's expectation of privacy. That the bank alter the form in which it records the information transmitted to it by the depositor to show the receipt and disbursement of money on a bank statement does not diminish the depositor's anticipation of privacy in the matters which he confides to the bank. A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.

* * * * * * *

"The People assert that no illegal search and seizure occurred here because the bank voluntarily provided the statements to the police, and the bank rather than the police conducted the search of its records for papers relating to petitioner's accounts. If, as we conclude above, petitioner has a reasonable expectation of privacy in the bank statements, the voluntary relinquishment of such records by the bank at the request of the police does not constitute a valid consent by this petitioner. . . . It is not the right of privacy of the bank but of the petitioner which is at issue, and thus it would be untenable to conclude that the bank, a neutral entity with no significant interest in the matter, may validly consent to an invasion of its depositors' rights. However, if the bank is not neutral as for example where it is itself a victim of the defendant's suspected wrongdoing, the depositor's right of privacy will not prevail.

"Our rationale is consistent with the recent decision of United States v. Miller (5th Cir. 1974), 500 F. 2d 751. In *Miller*, the United States Attorney, without the defendant's knowledge, issued subpoenas to two banks in which the defendant maintained accounts, ordering the production of 'all records of accounts' in the name of the defendant. The banks voluntarily provided the government with copies of the defendant's checks and a deposit slip; these items were introduced into evidence at the trial which led to his conviction. The circuit court reversed the conviction. It held that the defendant's rights under the Fourth Amendment were violated by the search because the subpoena was issued by the United States Attorney rather than by a court or grand jury, and the bank's voluntary compliance with the subpoena was irrelevant since it was the depositor's right to privacy which was threatened by the disclosure.

"We hold that any bank statements or copies thereof obtained by the sheriff and prosecutor without the benefit of legal process were acquired as the result of an illegal search and seizure (Cal. Const., art. I, § 13), and that the trial court should have granted the motion to suppress such documents.

* * * * * * *

"The underlying dilemma in this and related cases is that the bank, a detached and disinterested entity, reliquished the records voluntarily. But that circumstance should not be crucial. For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs

upon the reasonable assumption that the information would remain confidential. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.

"Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices." 13 Cal. 3d, at 243–248, 529 P. 2d, at 593–596, 118 Cal. Rptr., at 169–172 (footnote omitted).

The California Supreme Court also addressed the question of the relevance of *California Bankers Assn.* v. *Shultz*, 416 U.S. 21 (1974). In my view, for the reasons stated in *Burrows*, the decision of the Court of Appeals under review today, is in no way inconsistent with *California Bankers*.[12] The court said:

"[*California Bankers*] held, in a six-three decision, that the bank's rights under the Fourth Amendment were not abridged by the regulation, and that the depositor plaintiffs lacked standing to challenge the reporting requirement because there was no showing that they engaged in the type of transaction to which the regulation referred.

"The concurring views of two justices who provided the necessary votes to create a majority are of particular interests. Justice Powell's opinion, joined by Justice Blackmun, [416 U.S., at 78,] makes clear that a significant extension of the reporting requirement would pose substantial constitutional questions, and that concurrence with the majority was based upon the provisions of the act as narrowed by the regulations. He wrote, 'In their full reach, the reports apparently authorized by the open-ended language of the Act touch upon intimate areas of an individual's personal affairs. Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process. In such instances, the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate. United States v. United States District Court, 407 U.S. 297, 316–317.' [416 U.S., at 78–79.]

"Justices Douglas and Marshall dissented on the ground that the act violated the Fourth Amendment. Justice Brennan also filed a dissent, stating that the recordkeeping and reporting requirements of the act constituted an impermissibly broad grant of power to the Secretary.

". . . [T]he only federal case decided after *Shultz* and directly confronting the issue of the depositor's rights is entirely consistent with the views we have set forth above . . . *Miller* holds that *Shultz* may not be interpreted as 'proclaiming open season on personal bank records' or as permitting the government to circumvent the Fourth Amendment by first requiring banks to copy their depositors' checks and then calling upon the banks to allow inspection of those copies without appropriate legal process." 13 Cal. 3d, at 246–247, 529 P. 2d, at 595–596, 118 Cal. Rptr., at 171–172 (footnote omitted).

I would therefore affirm the judgment of the Court of Appeals. I add only that *Burrows* strikingly illustrates the emerging trend among high state courts

---

[12] I continue to believe that the reporting and recordkeeping requirements of the Bank Secrecy Act are unconstitutional. *California Bankers Assn.* v. *Shultz*, 416 U.S. at 91 (BRENNAN, J., dissenting). But I disagree with the Court's reasoning in this case even assuming the constitutionality of the Act, and therefore it is unnecessary for me to rely on the infirmities inherent in the Act.

of relying upon state constitutional protections of individual liberties[13]—protections pervading counterpart provisions of the United States Constitution, but increasingly being ignored by decisions of this Court. For the most recent examples in this Court, but only in the privacy and Fourth Amendment areas, see, *e.g.*, *Kelley* v. *Johnson*, 425 U.S.—(1976); *Doe* v. *Commonwealth's Atty.*, 425 U.S.—(1976); *Paul* v. *Davis*, 424 U.S.—(1976); *United States* v. *Watson*, 423 U.S.—(1976).

MR. JUSTICE MARSHALL, DISSENTING

In *California Bankers Assn.* v. *Shultz*, 416 U.S. 21 (1974), the Court upheld the constitutionality of the recordkeeping requirement of the Bank Secrecy Act. 12 U.S.C. § 1829b (d). I dissented, finding the required maintenance of bank customers' records to be a seizure within the meaning of the Fourth Amendment and unlawful in the absence of a warrant and probable cause. While the Court in *California Bankers Assn.* did not then purport to decide whether a customer could later challenge the bank's delivery of his records to the Government pursuant to subpoena, I warned:

"[I]t is ironic that although the majority deems the bank customers' Fourth Amendment claims premature, it also intimates that once the bank has made copies of a customer's checks, the customer no longer has standing to invoke his Fourth Amendment right when a demand is made on the bank by the Government for the records. . . . By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of records, the majority engages in a hollow charade whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late." 416 U.S., at 97 (dissenting op.).

Today, not surprisingly, the Court finds respondent's claims to be made too late. Since the Court in *California Bankers Assn.* held that a bank, in complying with the requirement that it keep copies of the checks written by its customers, "neither searches nor seizes records in which depositor has a Fourth Amendment right," 416 U.S., at 54, there is nothing new in today's holding that respondent has no protected Fourth Amendment interest in such records. *A fortiori*, he does not have standing to contest the Government's subpoena to the bank. *Alderman* v. *United States*, 394 U.S. 165 (1969).

I wash my hands of today's extended redundancy by the Court. Because the recordkeeping requirement of the Act orders the seizure of customers' bank records without a warrant and probable cause, I believe the Act is unconstitutional and that respondent has standing to raise that claim. Since the Act is unconstitutional, the Government cannot rely on records kept pursuant to it in prosecuting bank customers. The Government relied on such records in this case and, because of that, I would affirm the Court of Appeals' reversal of respondent's conviction. I respectfully dissent.

Lawrence G. Wallace, Deputy Solicitor General (Robert H. Bork, Solicitor General, Richard L. Thornburgh, Assistant Attorney General, Robert B. Reich,

---

[13] See, *e.g.*, cases cited in *Baxter* v. *Palmigiano*, slip op., at 16 and n. 10 (BRENNAN, J., dissenting); *Michigan* v. *Mosley*, 423 U.S. 96, 120–121 (1975) (BRENNAN, J., dissenting). See also Wilkes, The New Federalism in Criminal Procedure: State Court Evasion of the Burger Court, 62 Ky. L. J. 421 (1974); Wilkes, More on the New Federalism in Criminal Procedure, 63 Ky. L. J. 873 (1975); Falk, The State Constitution: A More Than "Adequate" Nonfederal Ground, 61 Cal. L. Rev. 273 (1973); Project Report, Toward an Activist Role for State Bills of Rights, 8 Harv. Civ. Rights-Civ. Lib. L. Rev. 271 (1973). In the past, it might have been safe for counsel to raise only federal constitutional issues in state courts, but the risks of not raising state law questions are increasingly substantial, as revealed by a colloquy during argument in *Michigan* v. *Mosley*, *supra:*

"QUESTION. Why can't you argue all of this as being contrary to the law and the Constitution of the State of Michigan?

"MR. ZIEMBA. I can because we have the same provision in the Michigan Constitution of 1963 as we have in the Fifth Amendment of the Federal Constitution, certainly.

"QUESTION. Well, you argued the whole thing before.

"MR. ZIEMBA. In the Court of Appeals?

"QUESTION. Yes.

"MR. ZIEMBA. I really did not touch upon—I predicated my entire argument on the Federal Constitution, I must admit that. I did not mention the equivalent provision of the Michigan Constitution of 1963, although I could have. And I may assure this Court that at every opportunity in the future, I shall. [Laughter.]

"QUESTION. But you hope you don't have that opportunity in this case.

"MR. ZIEMBA. That's right." Tr. of Oral Arg. 43–44.

It would be unwise for counsel to rely on state courts to consider state law questions *sua sponte*. But see *State* v. *Johnson*, 68 N.J. 349, 346 A. 2d 66 (1975).

Assistant to the Solicitor General, Sidney M. Glazer and Ivan Michael Schaeffer, Justice Dept. attorneys, with him on the brief) for petitioner; Denver Lee Rampey, Jr., Warner Robins, Ga. (Nunn, Geiger, Rampey, Buice & Harrington, with him on the brief) for respondent.

CLARENCE M. DITLOW, APPELANT

v.

GEORGE P. SCHULTZ, SECRETARY, DEPARTMENT OF THE TREASURY

No. 74–1975

UNITED STATES COURT OF APPEALS, DISTRICT OF COLUMBIA CIRCUIT

ARGUED JUNE 17, 1975—DECIDED AUG. 11, 1975

Action was brought pursuant to Freedom of Information Act (FOIA) seeking declaratory and injunctive relief requiring the Secretary of the Department of the Treasury to produce and make available for copying and inspection certain United States customs declaration forms. The United States District Court for the District of Columbia, 379 F. Supp. 326, Joseph C. Waddy, J., granted summary judgment for the Secretary and the plaintiff appealed. The Court of Appeals, Leventhal, Circuit Judge, held that where the plaintiff did not desire disclosure of the requested information unless a related antitrust action was determined to be maintainable as a class action and where the antitrust action had been dismissed by the district court, the Court of Appeals would defer ruling on difficult questions presented by the merits of the present FOIA appeal pending further developments in the antitrust appeal. The Court of Appeals found appellant's challenge to the district court's dismissal of the FOIA action sufficiently substantial to warrant an order requiring the Secretary of the Treasury to preserve the requested information pending resolution of the appeal.

Decision deferred.

Circuit Judge Robb would affirm the judgment of the District Court, without more.

1. Records ⇐ 14

In order to justify denial of plaintiff's request of information furnished on customs declaration forms based on exemption of the Freedom of Information Act for personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, the Secretary of the Treasury would be required to show both that the material sought qualifies as a personnel, medical, or similar file and that disclosure would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C.A. § 552(b)(6).

2. Records ⇐ 14

The Freedom of Information Act creates a liberal disclosure requirement, limited only by specific exemptions which are to be narrowly construed. 5 U.S.C.A. § 552.

3. Records ⇐ 14

The "clearly unwarranted invasion of personal privacy" language within exemption to the Freedom of Information Act expresses a carefully considered congressional policy favoring disclosure which instructs the court to tilt the balance in favor of disclosure. 5 U.S.C.A. § 552(b)(6).

4. Records ⇐ 14

Evidence did not support district court's finding that plaintiff, who sought information furnished on customs declaration forms by trans-Pacific passengers for purpose of bringing antitrust class action against airlines, had available sources of information which might suffice other than the government files which the plaintiff sought under the Freedom of Information Act, 5 U.S.C.A. § 552(b)(6).

5. Courts 406.9(1)

Where the plaintiff did not seek disclosure of the requested information unless a related antitrust action was determined to be maintainable as a class action

and where the antitrust action had been dismissed by the district court, the Court of Appeals would defer ruling on difficult questions presented by the merits of the present FOIA appeal pending further developments in the antitrust action. 5 U.S.C.A. § 552(b)(4, 6).

Appeal from the United States District Court for the District of Columbia (D.C. Civil Action 74-302).

Girardeau A. Spann, Washington, D.C., for appellant. Larry P. Ellsworth, Washington, D.C., was on the brief for appellant. Alan B. Morrison, Washington, D.C., also entered an appearance for appellant.

Paul Blankenstein, Atty., Dept. of Justice, with whom Irving Jaffe, Acting Asst. Atty. Gen., Earl J. Silbert, U.S. Atty., and Leonard Schaitman, Atty., Dept. of Justice, were on the brief for appellee. Thomas G. Wilson, Atty., Dept. of Justice, also entered an appearance for appellee.

Before LEVENTHAL and ROBB, *Circuit Judges*, and MERHIGE,* *United States District Judge* for the Eastern District of Virginia.

Opinion for the Court filed by *Circuit Judge* LEVENTHAL.

LEVENTHAL, *Circuit Judge:*

I.

This case involves a Freedom of Information Act (FOIA) action brought to obtain the name, address, and flight number information in the Government's files of Customs Declarations Forms 6059–B, forms completed by travelers returning to the United States.

Appellant Clarence M. Ditlow proposes to use these data to assemble a list of class members in conjunction with an antitrust class action he has filed alleging overcharges by ten airlines on flights to the United States from points in the Transpacific airline market between May 1, 1973, and September 1, 1973.[1] In the present FOIA action, he seeks an order requiring the Secretary of the Treasury to safeguard the forms against destruction to assure their availability for later use in identifying the antitrust class [2] and a declaratory ruling that he is entitled to the requested information when and if the class is certified.[3]

Prior to bringing this action, appellant wrote the Commissioner of Customs requesting the name and address information from pertinent 6059–B forms. The Bureau of Customs denied the request on the grounds that the information was exempt from disclosure under the (b)(4), commercial and financial information, and (b)(6), personal privacy, exemptions of the FOIA. The Commissioner stated that he "fully considered the advisability of making a discretionary disclosure" of the requested data but decided "against discretionary disclosure . . . based upon our policy of protecting the right of privacy of international travelers." [4]

The District Court granted the Secretary's motion for summary judgment, finding that although the (b)(4) exemption was inapplicable, the information came within the (b)(6) exemption of files the disclosure of which would result in

---

*Sitting by designation pursuant to 28 U.S.C. § 292(d).

[1] No. 999–73 (D.D.C., filed May 22, 1973). The District Court entered an order granting the defendant airlines summary judgment on April 25, 1975. The plaintiff has appealed this order. *See* text at notes 28–29 *infra*.

[2] Appellant indicates that the 6059–B forms are ordinarily destroyed one year after they are obtained. *See* Brief for Appellant at 5 *citing* Levine v. United States, No. 73–1315, slip op. at 5 (S.D. Fla., Mar. 22, 1974). By letter of October 9, 1974, appellee consented to preserve the customs declarations involved in this action pending resolution this case. *See* Letter from Arnold T. Aikens, Chief, Civil Division, to Raymond T. Bonner, Oct. 9, 1974, *reprinted at* Brief for Appellant at a–15.

[3] *See* Brief for Appellant at 15. In his requests to the Bureau of Customs and his papers in the District Court, appellant's attempt to obtain disclosure of the name, address, and flight number data was not conditioned on certification of the antitrus class. *See* JA 8–9 (Letter from Raymond T. Bonner to Regional Commissioners of Customs, May 24, 1973), JA 2–4 (Complaint in No. 74–302, D.D.C., filed Feb. 15, 1974).

[4] JA 16. By letter of May 24, 1973, appellant requested data from the 6059–B forms from the Regional Commissioners of Customs in Los Angeles and San Francisco (JA 8–9). That request was denied on the grounds that the "declarations contain commercial or financial information which is exempt from disclosure under the provisions of 5 U.S.C. 552(b)(4) and section 103.7(d) of the Customs Regulations." Letter from Leonard Lehman, Assistant Commissioner of Customs, to Raymond T. Bonner, July 31, 1973. (JA 10). Next appellant appealed this denial to the Commissioner of Customs. On August 27, 1973, the Commissioner denied the appeal, stating that the material came within both the (b)(4) commercial or financial information exemption and the (b)(6) privacy exemption. Letter from Vernon D. Acree to Raymond T. Bonner. (JA 12–13). Before filing this action, appellant again wrote Commissioner Acree seeking disclosure. The Commissioner remained steadfast in his view that release of the data would violate exemption 6 and he declined to make a discretionary disclosure to appellant. Letter from Vernon D. Acree to Raymond T. Bonner, Feb. 11, 1974. (JA 16).

a "clearly unwarranted invasion of personal privacy." [5] More specifically, the court concluded that disclosure of the names and addresses "would constitute a substantial invasion of privacy" and that there were "other sufficient sources of information." [6] Plaintiff Ditlow appealed from the summary judgment ruling.

II.

[1–3] The sole issue on appeal is the validity of the District Court's determination that the requested material is exempt under 5 U.S.C. § 552(b)(6) (1970). That section provides:

> (b) This section does not apply to matters that are—
>
> (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

In order to justify denial of appellant's request based on exemption 6, the Secretary must show both that the material sought qualifies as a personnel, medical, or similar file and that disclosure would constitute a "clearly unwarranted invasion of personal privacy." [7] In ruling on FOIA appeals, we are mindful that the Act "creates a liberal disclosure requirement, limited only by specific exemptions which are to be narrowly construed." [8] In addition to the Act's general presumption of disclosure, the "clearly unwarranted invasion of personal privacy" language expresses "a carefully considered congressional policy favoring disclosure" which "instructs the court to tilt the balance in favor of disclosure." [9]

This case presents a number of difficult questions concerning the interpretation and implementation of exemption 6. We shall sketch some of these problems. An initial issue is whether the requested material qualifies as a "similar file" since it clearly is neither a personnel nor a medical file. Our *Rural Housing* decision noted that the (b)(6) "exemption was designed to protect individuals from public disclosure of intimate details of their lives" and concluded that the "similar files" language was intended "broadly to protect individuals from a wide range of embarrassing disclosures." [10] The District Court determined that the completed customs forms including the travelers' "names, ages, citizenship, residency, permanent addresses, addresses while in the United States, the names and relationship of family members, personal finances, when and where their visas were issued, and all acquisitions while abroad, including the price thereof" constituted "similar files." [11] In reviewing that determination, we not only are faced with evaluating whether this information includes " 'intimate details' of a 'highly personal nature' " but are also confronted with the question whether the entire form or merely the requested name, address, and flight number information must be adjudged a similar file for the exemption to be invoked.[12]

---

[5] Ditlow v. Shultz, 379 F. Supp. 326 (D.D.C. 1974).

[6] *Id.* at 331.

[7] *See, e.g.*, Wine Hobby USA, Inc. v. IRS, 502 F. 2d 133, 135 (3d Cir. 1974) ; Rural Housing Alliance v. Dept. of Agriculture, 162 U.S. App. D.C. 122, 126, 498 F. 2d 73, 77 (1974) ; Getman v. NLRB, 146 U.S. App. D.C. 209, 213, 450 F. 2d 670, 674, *stay denied*, 404 U.S. 1204, 92 S. Ct. 7, 30 L. Ed. 2d 8 (1971) (Black, Acting Circuit Justice) ; Note, *The Freedom of Information Act: A Seven-Year Assignment*, 74 *Colum. L. Rev.* 895, 953 (1974).

It is well established that the governmental agency has the burden of establishing that the requested material comes within one of the exceptions. *See* Robles v. EPA, 484 F. 2d 843, 845 (4th Cir. 1973) ; Getman v. NLRB, *supra*, at 213, 450 F. 2d at 774.

[8] *See* Bristol-Myers Co. v. FTC, 138 U.S. App. D.C. 22, 25, 424 F. 2d 935, 938 (1970).

[9] Getman v. NLRB, *supra* note 7, at 213 and n. 4, 450 F. 2d 674 and n. 4.

[10] 162 U.S. App. D.C. at 126, 498 F. 2d at 77 ; *see* Robles v. EPA, *supra* note 7, 484 F. 2d at 845 ; *cf.* Getman v. NLRB, *supra* note 7, at 214, 450 F. 2d at 675 (Although the *Getman* court assumed *arguendo* that a "similar file" was involved, it noted that "the real thrust of Exemption (6) is to guard against unnecessary disclosure of files . . . which would contain intimate details' of a 'highly personal' nature."). *But cf.* Wine Hobby USA, Inc. v. IRS, *supra* note 7, 502 F. 2d at 135 (reading "similar files" to include any file containing information of a personal quality and finding that the "term similar' was [not] intended to narrow the exemption from disclosure.").

[11] 379 F. Supp. at 329.

[12] The District Court made no reference to the possibility that the relevant 'file" for purposes of the Act may be one limited to information showing the name, address, and flight number of the travelers returning to the United States from the Transpacific area during the four-month period, May 1–Sept. 1, 1973. It is doubtful that such a limited file can fairly be deemed one having the quality of intimate or highly personal details. *See* notes 14–15 and text thereto. One can speculate instances in which disclosure of such information might prove embarrassing—*e.g.*, to a traveler who for personal or commercial reasons has put forward a different account of his activities. There may likewise be occasions where a telecast of the crowd at a baseball game may show and embarrass the employee who sought and obtained time off for his grandmother's funeral. The issue is whether the nature of the file and of the privacy interest (in the linkage of name and home address to the "public" appearance of the traveler on the aircraft) is such as to render this a "similar file", with public disclosure constituting a 'clearly unwarranted invasion of personal privacy."

A related question is whether any potential privacy infringement, no matter how slight or speculative, serves to trigger the exemption absent a counterbalancing public interest in disclosure or whether a threatened exposure of intimate or embarrassing personal details is necessary as a threshold matter before the court proceeds to a balancing of private and public interests. The *Rural Housing* court indicated that the exemption was directed at "intimate details" such as "marital status, legitimacy of children, identity of fathers of children, medical condition, welfare payments, alcoholic consumption, family fights, reputation, and so on." [13] However, our *Getman* decision engaged in a balancing of interests even though the disclosure of names and addresses of certain union members in that case was deemed not "embarrassing" and threatened privacy only "to a very minimal degree." [14] The invasion of privacy in this case is roughly similar to that in *Getman*—names and addresses are sought along with information that the individual returned to the United States from Asia or Australia by air sometime between May 1 and September 1, 1973.[15] Although a not clearly inconsequential loss of privacy would be occasioned here, disclosure would result in less than a substantial invasion of privacy.

Assuming *arguendo* that sufficient privacy concerns are implicated by appellant's disclosure requests to warrant a balancing of competing interests, we are required to ascertain exactly what privacy loss and public interest are to be balanced. In Getman and Rural Housing, this court has weighed the privacy loss from disclosure to the requesting party against "the public interest purpose *of those seeking disclosure*, and whether other sources of information might suffice." [16] This formulation appears to assume, as *Getman* stated in footnote, that exemption (6) contemplates "an implicit limitation that the information, once disclosed, be used only by the requesting party and for the public interest purpose upon which the balancing was based." [17] Under such an assumption the privacy loss would be narrowed by the nature of the requesting party and its proposed use of the information and the public interest factor would be limited to the purposes served by that use. We believe that there is a substantial question whether Congress contemplated this limited balancing approach or whether the court has any independent equity authority to fashion a restrictive disclosure order.[18] We cannot blink the wording of the central provision, 5 U.S.C. § 552,

---

[13] 162 U.S. App. D.C. at 126, 498 F. 2d at 77.

[14] 146 U.S. App. D.C. at 214, 450 F. 2d at 675. *Rural Housing* indicates that intimate of highly personal details must be involved in (order to satisfy the "similar files" predicate to the balancing test required to ascertain whether disclosure would result in a "clearly unwarranted invasion of personal privacy." *Getman* appears to have engaged in a balancing in a case involving a relitvely minor loss of privcy only because it assumed *arguendo* that the 'similar files" predicate was met.

[15] In *Getman* the disclosure of names and addresses of union members was deemed a relatively minor loss of privacy. There the context of the disclosure of names and addresses also revealed the type of work the individual did, the person's employer, whether the person was a union member, and the union to which the individual belonged. Disclosure exposed those persons to a telephone request that they consent to a probing interview on union election procedures. Here the information—the individual's name and address and the fact that he returned to the United States by air from Asia or Australia between May 1 and September 1, 1973—comprises at least no greater an invasion of privacy. The only consequence of the exposure here is a mailed notice informing the person that he is a member of a class and may be awarded damages for airline overcharges.

In Wine Hobby, Inc. v. IRS, 502 F. 2d 133 (3d Cir. 1974), the Third Circuit found that disclosure of names and addresses of heads of families who produce "for family use and not for sale an amount of wine not exceeding 200 gallons per annum" would constitute an invasion of privacy. *Id.* at 134, 137. The court stated that the requested material not only revealed name and address information but also "family status of the registrant, including the fact that he is not living alone and that he exercise family control or responsibility in the household" and the fact that wine-making activities are being conducted within the home. *Id.* at 137. The court made no assessment of the seriousness of the privacy loss threatened by such disclosures other than observing that "the invasion of privacy in this case is not as serious as that considered by the court in other cases." *Id.*; *see* 16 *B.C. Ind. & Com.* L. Rev. 240, 251 (1975) (concluding that such disclosures "would result in only a minor invasion of personal privacy"). No assessment was required because the requesting party "advanced no direct or indirect public interest purpose in disclosure of these lists" and the court itself could "conceive of none." 502 F. 2d at 137. Given the absence of any perceived public interest in disclosure, the court concluded that the invasion of privacy would be "clearly unwarranted." *See* note 25 *infra*.

[16] *See* Rural Housing Alliance v. Dept. of Agriculture, *supra* note 7, at 126, 498 F. 2d at 77; Getman v. NLRB, *supra* note 7, at 214, 450 F. 2d at 675 (emphasis added).

[17] *See* 146 U.S. App. D.C. at 216 n. 24, 450 F. 2d at 677 n. 24.

[18] We have held that the courts do not "have equitable discretion to permit withholding of information which does not fall within one of the specific exemptions to the Act." Getman v. NLRB, *supra* note 7, at 216, 450 F. 2d at 677. *Accord* Robles v. EPA, *supra* note 7, 484 F. 2d at 847; Soucie v. David, 145 U.S. App. D.C. 144, 154, 448 F. 2d 1067, 1077 (1971); Wellford

stating that "[e]ach agency shall make available *to the public* information" set forth in subsection (a), if the exemptions listed in subsection (b) are inapplicable. And the critical Senate Report states that application of the exemption "will involve a balancing of interests between the protection of an individual's private affairs from unnecessary *public* scrutiny, and the preservation of the *public's* right to governmental information."[19] That a balancing is envisioned is plain.[20] What is unclear is whether the balancing is to be performed in the context of unrestricted disclosure to the public or of a use-specified release confined to the requesting parties.[21]

Further questions are raised in this case regarding the weight of privacy interests threatened by and the public interests served by disclosure. It is unclear what effect the absence of a governmental assurance of confidentiality to the travelers completing the customs forms and the Bureau of Customs' apparent assertion of authority to make discretionary disclosure of the information have on the evaluation of the threat to privacy. Both of these factors would seem to undercut the privacy expectations protected by exemption 6.[22]

As to the second half of the balancing test, the Government contends that the public interest promoted by disclosure must relate to "the basic concern of the Act . . . to make available the legitimate information that an informed electorate needs to properly monitor the activities of the federal government." The Secretary contends that appellant's asserted interest in facilitating a private action to enforce the antitrust laws falls outside the public interest purpose of the FOIA since it does not involve an evaluation of governmental performance.[23] While we are doubtful that the public interest considerations can be limited to those at the core of the Act, the Secretary's argument at least requires us to consider whether the more general public interest in disclosure asserted by appellant should be given less weight than an interest in obtaining information

---

v. Hardin, 444 F. 2d 21, 24–25 (4th Cir. 1971). *But see* Consumers Union v. Veterans Administration, 301 F. Supp. 796 (S.D.N.Y. 1969), *appeal dismissed as moot*, 436 F. 2d 1363 (2d Cir. 1971). K. Davis, Administrative Law Treatise § 3A.6 at 123–24 (1970 Supp.); *cf.* GSA v. Benson, 415 F. 2d 878, 880 (9th Cir. 1969). Therefore, unless the (b)(6) exemption itself intended to modify the "any person" language of § 552(a)(3) and to permit restriction of disclosure to the requesting party and his proposed use, the court would appear to be without authority to impose such limitations through an exercise of equitable discretion.

[19] S. Rep. No. 813, 89th Cong., 1st Sess. 9 (1967) (emphasis added). The phrasing of the House Report suggests that the "clearly unwarranted invasion of personal privacy" limitation reflects a balance struck by Congress between privacy and public interests. *See* H. Rep. No. 1497, 89th Cong., 2d Sess. 11 (1967) ("The limitation of a 'clearly unwarranted invasion of personal privacy' provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to Government information by excluding those kind of files the disclosure of which might harm the individual.") The House Report may be read as indicating that the courts are only to assess the degree of the privacy invasion and are not to engage in their own case by case balancing of the private and public interests. *See* Note, *Invasion of Privacy and the Freedom of Information Act:* Getman v. NLRB, 40 Geo. Wash. L. Rev. 527, 535–36 and nn. 48–49 (1972). However, courts and commentators have concluded that the Senate Report "is to be preferred over the House report as a reliable indicator of legislative intent because the House report was not published until after the Senate had already passed its bill." *See* Getman v. NLRB, *supra* note 7, at 212 n. 8, 450 F. 2d at 673 n. 8 and sources cited thereat.

[20] *But see* Note, *Supra* note 19, at 534.

[21] *Getman* argues that, "[s]ince Exemption (6) necessarily requires the court to balance a public interest purpose for disclosure of personal information against the potential invasion of individual privacy", the exemption must intend to restrict disclosure to the requesting party and the proposed use. 146 U.S. App. D.C. at 216 n. 24, 450 F. 2d at 677 n. 24. However, the passage from the Senate Report relied upon in *Getman* refers to protection against "public scrutiny" and to "the public's right to governmental information" rather than to the privacy risk from disclosure to a particular requesting party or the specific public interest served by that party's proposed use of the material. A general balancing of the privacy loss from release to the public and the public interest in disclosure to the public would carry out the discernible intent of the Senate Report without conflicting with the Act's broad purpose to enable "any person" to request disclosure without making a showing that he was "properly and directly concerned with the information. *See* H. Rep. No. 1497, *supra* note 19, at 1, 6, 8; S. Rep. No. 813, *supra* note 19, at 5; Robles v. EPA, *supra* note 7, 484 F. 2d at 847 and n. 6 *quoting K. Davis*, *supra* note 19, at 120–21; Sterling Drug, Inc. v. FTC, 146 U.S. App. D.C. 237, 243–44 n. 4, 450 F. 2d 698, 704–05 n. 4 (1971) (noting that the "any person" language of the Act precluded an examination of "the applicant's need" for the information). While the selectivity provided by the *Getman* approach might be desirable from a policy standpoint as allowing a more refined harmonizing of privacy and disclosure interests, it is questionable whether Congress intended to create such a broad exception to the "any person" provision by adopting the "clearly unwarranted" language of exemption 6. The interest in disclosure to the public may be characterized by showing the uses contemplated by some members of the public specifically, but not exclusively, the plaintiffs.

[22] *See* Robles v. EPA, *supra* note 7, 484 F. 2d at 846 (noting that a promise of confidentiality is "a factor to be considered" and finding "important" the "fact that the information" requested had been readily made available upon request).

[23] Brief for Appellee at 26–29.

material for monitoring the Government's activities.[24] Moreover, even if we were to accept the Government's argument, appellant's antitrust action might well be viewed as involving an indirect criticism of the performance of the CAB in protecting the public against anticompetitive activities of regulated air carriers.[25]

[4] A final aspect of the balancing approach contained in *Getman* and *Rural Housing* is whether "other sources of information might suffice."[26] The District Court erroneously stated that "[p]laintiff recognizes the availability of other sufficient sources of information." The court's discussion indicates that only "some of the information" is available from passenger lists, reservation records, and credit card records retained by the airlines.[27] It is clear, however, that name and address information is available from nongovernmental sources only for those passengers whose tickets were mailed to them by the airlines or who paid for their flights by credit card.[28] In these circumstances, discovery from the defendants in the antitrust action would not "suffice" to meet appellant's potential need for a complete list of names and addresses of class members.

[5] However, although there is no other sufficient source of information, there appears to be an alternative to the use of the FOIA to obtain the data.[29] Instead of bringing this FOIA action, appellant could have subpoenaed the customs forms from the Bureau under Rule 45(b), Fed.R.Civ.P. The discovery motion might well have prompted the same objections that the Secretary has pressed in resisting the FOIA request. If disclosure under the FOIA can be restricted to the requesting party and his proposed use, there would not be a significant difference between the two methods of securing the information. On the other hand, if an FOIA action results in disclosure to the public at large, the discovery approach would avoid unnecessary infringement of privacy interests by confining disclosure to sue by the parties in the antitrust litigation. The existence of the discovery alternative raises a question as to whether resort to the FOIA is appropriate where the information is sought in connection with ongoing litigation.[30]

In view of the peculiar circumstances of the present appeal, we do not believe that it is either a necessary or an appropriate allocation of judicial resources to resolve these difficult questions at this time. Appellant does not even desire disclosure of the requested information unless his antitrust action is determined to be maintainable as a class action. It is quite possible that the antitrust action will never reach that stage and thus that resolution of the FOIA claim will have no impact on the parties to this appeal, the parties to the antitrust action, or the individuals who completed the requested customs forms. The antitrust complaint was filed on May 22, 1973, and dismissed by the District Court pursuant to the defendants' motion on August 7, 1973. This court vacated the District Court's judgment on October 30, 1974, and remanded the case with "instructions to retain jurisdiction while directing the parties to take appropriate action before the Civil Aeronautics Board." The court directed this course because of its view that "the first critical, and perhaps dispositive issue in the case is: What fares over the Pacific, those ceasing 31 March 1973 or those to be effective through 30 April 1973, if any, were in effect during May 1973?" and that "this is an issue which should be decided in the first instance by the Civil Aeronautics Board." After the CAB issued a declaratory order stating that the April 1973 rates were in effect through late July 1973, the District Court granted summary judgment to the defendants.

---

[24] This core purpose is reflected in the legislative history to the 1974 amendments to the FOIA, referring to the 1966 Act as "milestone law [which] guarantees the right of persons to know about the business of their government" and noting that the amendments are designed "to reach the goal of more efficient, prompt, and full disclosure of information." *See* H. Rep. No. 876, 93d Cong., 2d Sess. 4–5, U.S. Code Cong. & Admin. News, p. 6271 (1974).

[25] This case is clearly distinguishable from *Wine Hobby* where the only interest in disclosure asserted by the requesting party was stipulated to be private commercial exploitation and no direct or indirect public interest purpose was advanced by the requesting party or discerned by the court. 502 F. 2d at 137.

[26] *See* 162 U.S. App. D.C. at 126–27, 498 F. 2d at 77–78; 146 U.S. App. D.C. at 214, 215–16, 450 F. 2d at 675, 676–77.

[27] 379 F. Supp. at 331. (emphasis added.)

[28] Brief for Appellee at 30.

[29] Both *Getman* and *Rural Housing* focused on the availability of nongovernmental sources of the requested information rather than other means of obtaining the data from the agency. *See* note 25, *supra*.

[30] *Cf.* Kerr v. United States District Court, 511 F. 2d 192, 197–98 (9th Cir. 1975); Secretary of Labor v. Farino, 490 F. 2d 885, 893 (7th Cir. 1973).

We conclude that appellant's challenge to the District Court's dismissal of his FOIA action is sufficiently substantial to warrant an order requiring the Secretary of the Treasury to preserve the requested customs forms to avoid mooting the case. Should this court find that the trial judge erred in granting summary judgment in the antitrust action and should the District Court certify that the antitrust suit is properly maintainable as a class action, appellant may reactivate this FOIA appeal. We defer the merits of the appeal pending such future developments and order that appellee take appropriate steps to preserve the requested information pending resolution of this appeal.[31]

So ordered.

Circuit Judge ROBB would affirm the judgment of the District Court, without more.

CLARENCE M. DITLOW, PLAINTIFF

v.

GEORGE P. SHULTZ, SECRETARY, DEPARTMENT OF THE TREASURY, DEFENDANT

Civ. A. No. 74–302

UNITED STATES DISTRICT COURT, DISTRICT OF COLUMBIA. JULY 19, 1974

Action was brought pursuant to Freedom of Information Act seeking declaratory and injunctive relief requiring the Secretary of the Department of Treasury to produce and make available for copying and inspection the United States Customs Declaration completed by all persons who entered the United States by air from certain areas in the transpacific air carrier market. Plaintiff moved for summary judgment and defendant moved to dismiss or, in the alternative, for summary judgment. The District Court, Waddy, J., held that with exception of names and addresses much of the information recorded on the forms fell within exclusionary clause of Act for privileged or confidential commercial or financial information, that forms also constituted "similar files" within meaning of exception for "personnel and medical files and similar files" but that even though documents constituted "similar files" they were still produceable unless their disclosure would constitute a clearly unwarranted invasion of personal privacy and that in making such determination the court was to balance the interests of the parties and that disclosure of names and addresses would constitute substantial invasion of privacy and, also, was unnecessary since such information could be dicovered by other methods.

Plaintiff's motion denied, defendant's motion for summary judgment granted.

1. Records ⇐ 14

Except for names and addresses, much of the information required by the Government and recorded on customs declaration form is confidential information that would not customarily be disclosed to the public by the person from whom it was obtained and, also public disclosure thereof imposes likelihood of harm to legitimate interests; such information falls within exclusion of Freedom of Information Act for privileged or confidential commercial or financial information. 5 U.S.C.A. § 552(b)(4).

2. Records ⇐ 14

When completed with information as to names, ages, citizenship, residency, personal finances, etc., the customs declaration form 6059–B contains intimate details of a highly personal nature and constitutes "similar files" within meaning of the exemption requirement of Freedom of Information Act for personnel and medical files and similar files, disclosure of which would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C.A. § 552(b)(6).

NOTE.—See publication Words and Phrases for other judicial constructions and definitions.

---

[31] This preservation order simply implements appellees' undertaking to "preserve the customs undertaking to "preserve the customs declarations involved in this suit . . . pending resolution of this case." *See* Letter from Arnold T. Aikens to Raymond T. Bonner, Oct. 9, 1974. There may be a limited housekeeping burden on the Government pendente lite, but this is not commensurate with the harm of a disclosure violating a statutory provision.

3. Records ⇐ 14

Even through documents constitute "similar files" within meaning of exemption of Freedom of Information Act for personnel and medical files and similar files, such documents are produceable unless their disclosure constitute a clearly unwarranted invasion of personal privacy; in making such determination the court must exercise its discretion by balancing the interests of the parties, i. e., the right of the public to have access to government information, including the reasons for the particular request for the documents at issue, against the right of personal privacy of the affected individuals. 5 U.S.C.A. § 552(b)(6).

4. Records ⇐ 14

Neither names and addresses nor other information furnished on customs declaration forms were required to be disclosed to plaintiff, who sought names and addresses of passengers who flew in the transpacific market for purpose of maintaining class action charging air carriers with violating antitrust law as regards air fares, since not only would disclosure of names and addresses as well as other information constitute a substantial invasion of privacy but such disclosure was unnecessary since, even if antitrust complaint, which had been dismissed at trial level, were reinstated on appeal the desired information could be obtained by way of discovery. 5 U.S.C.A. § 552(b)(6).

Raymond T. Bonner and Ronald L. Plesser, Washington, D.C., for plaintiff.

Earl J. Silbert, U.S. Atty., Arnold T. Aikens and Eric B. Marcy, Asst. U.S. Attys., Washington, D.C., for defendant.

MEMORANDUM OPINION

WADDY, District Judge.

I.

This case is before the Court on the motion of plaintiff for summary judgment and defendant's motion to dismiss or in the alternative for summary judgment. This action is brought pursuant to the Freedom of Information Act, 5 U.S.C. § 552, and this Court has jurisdiction pursuant to 5 U.S.C. § 552(a)(3) of that Act. Plaintiff Ditlow seeks declaratory and injunctive relief, requiring defendant to produce and make available for copying and inspection the U.S. Customs Declaration (Customs Form 6059–B, November 1972) completed by all persons who entered the United States by air from points in Asia/Australia/Australasia between May 1, 1973, and September 1, 1974.

Plaintiff claims that he seeks the names and addresses appearing on the Customs Declarations "in order to fulfill his obligations as representative of the class of all passengers who were charged unlawful fares pursuant to the violations of law alleged in [another] action." The other action referred to by plaintiff is Civil Action 999–73 (D.D.C.), in anti-trust action brought by plaintiff against Pan American World Airways Inc., and nine other airlines engaged in the transportation of passengers in the transpacific market. In that action plaintiff seeks to recover on his own behalf the sum of $125.40 and three-fold damages for each person who flew via the defendants' airlines between points in the United States and points in Asia/Australia/Australasia and islands in the Pacific during the identified period. The case was dismissed by this Court on August 7, 1973 for failure to state a claim upon which relief can be granted under the Sherman Antitrust Act. It is currently pending before the United States Court of Appeals, D.C. Circuit, No. 73–1936.

The defendant, Secretary of the Department of the Treasury, under whose jurisdiction falls the Bureau of Customs, and who has custody of the requested documents, opposes disclosure of this information on the grounds that such information is specifically exempted by sections 552(b)(4) and (b)(6)[1] of the Freedom of Information Act.

---

[1] Section 552 of the FOIA provides, *inter alia*,

"(b) This section does not apply to matters that are—

* * * * * * *

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

* * * * * * *

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;"

II.

The material facts are these: all persons entering the United States are required to complete U.S. Customs Declaration form 6059–B, and these completed forms are kept in the possession of the Department of the Treasury. This form consists of one sheet of paper with inquiries on both sides. The front side requests the following information: (1) the name of the declarant; (2) the declarant's date of birth; (3) the vessel or airline and flight number on which the declarant arrived; (4) the declarant's citizenship; (5) residency; (6) permanent address; (7) address while in the United States; (8) the name and relationship of accompanying family members (9) whether or not declarant or anyone in declarant's party is carrying any agricultural or meat products or pets; (10) whether or not anyone is carrying over $5000 in coin, currency, or negotiable instruments; (11) a certification by declarant that all statements on the declaration are true, correct and complete; and, if declarant is a noncitizen, (12) requests the place his visa was issued and (13) the date it was issued. The back side of the form requests a detailed list of all articles acquired abroad which are in declarant's possession at the time of arrival, including price information on articles so acquired.

Plaintiff, through his attorney, requested access to the Customs Declaration forms in a letter to the regional commissioners of customs in Los Angeles and San Francisco, wherein plaintiff specified his particular interest in the names and addresses of the declarants. This request was denied by the Assistant Commissioner, Officer of Regulations and Rulings, Department of the Treasury, Bureau of Customs, on the ground that the "declarations contain commercial or financial information which is priveleged or confidential and, therefore, is exempt from disclosure under the provisions of 5 U.S.C. § 552(b)(4)" and parallel sections of the Customs Regulations. Plaintiff appealed this decision to the Comimssioner, Bureau of Customs, and emphasized that the only information sought off the forms was the names and addresses of the declarants. The appeal was denied.

In denying the appeal, the Commissioner of Customs re-asserted the view that the information requested was exempt from disclosure under the provisions of 5 U.S.C. § 552(b)(4), stating:

"We interpret the terms 'commercial or financial information' as used in the statute and in our regulations to include the fact of a person's arrival at a port in the United States from an overseas destination via a named air carrier, and we believe the fact of his arrival to be privileged or confidential."

5 U.S.C. § 552 (1970).

The Commissioner denied the appeal on the additional ground that "disclosure of the information requested would violate the right of personal privacy of the affected individuals, 5 U.S.C. 552(b)(6) . . ." and cited the case of Getman v. N.L.R.B., 146 U.S. App. D.C. 209, 450 F.2d 670, 674 (1971), wherein the Court stated that it is necessary "to balance the right of privacy of affected individuals against the right of the public to be informed." Again plaintiff appealed to the Commissioner, reiterating that he was seeking only the names and addresses which appear on the declarations, and requesting the Commissioner to reconsider his earlier denial in light of relevant judicial decisions handed down subsequent to the Commissioner's initial denal. Ths request was dened on the basis that the "information is confidential and exempt from disclosure under the provisions of 5 U.S.C. 552(b)(6)." No mention is made in this letter of any denial under 5 U.S.C. § 552(b)(4). Shortly thereafter the present action was filed.

III.

[1] With respect to Exemption (4) it appears to this Court that much of the information required by the Government and recorded on the Customs Declaration form is confidential information that would not customarily be disclosed to the public by the person from whom it was obtained and also that public disclosure of the information poses the likelihood of harm to legitimate private interests. Disclosure of such information is excluded by Exemption (4). *Cf.* National Parks and Conservation Ass'n v. Morton, D.S.Cir., 498 F.2d 765 (1974). However, bare disclosure of the names and addresses of the passengers is not precluded by Exemption (4) and might be disclosed unless nondisclosure is required by Exemption (6).

IV.

[2] Any holding that Exemption (6) is applicable to certain documents must be predicated on a finding that the subject documents are either "personnel", "medical" or "similar files" within the meaning of that Exemption. There is no contention that the documents plaintiff seeks in this case are "personnel" or "medical" files. On the question of what the term "similar files" means, the Court in *Getman* said:

"Both the House and Senate reports on the bill which became the Freedom of Information Act indicate that the real thrust of Exemption (6) is to guard against *unnecessary disclosure* of files of such agencies as the Veterans Administration or the Welfare Department or Selective Service or Bureau of Prisons, which would contain 'intimate details' of a 'highly personal' nature." (footnotes omitted) (emphasis supplied). 450 F.2d at 675. See also, Robles v. Environmental Protection Agency, 4 Cir., 484 F.2d 843, 845 (1973).

Although no promise of confidentiality was made at the time the information to complete Form 6059–B was obtained, the individuals entering the country were required by law to divulge information that they would not otherwise disseminate for general and public use. This information concerns their names, ages, citizenship, residency, permanent addresses, addresses while in the United States, the names and relationship of family members, personal finances, when and where their visas were issued, and all acquisitions while abroad, including the price thereof. This Court is of the opinion, and finds, that the Custom Declaration Form 6059–B, when completed with the above-mentioned information, contains "intimate details" of a "highly personal" nature and are "similar files" within the meaning of Exemption (6).

V.

[3, 4] Even though the documents in question are "similar files" within the meaning of Exemption (6), they are still producible unless their disclosure would constitute a "clearly unwarranted invasion of personal privacy." The Court of Appeals in *Getman* stated that the ". . . statutory language 'clearly unwarranted' instructs the court to tilt the balance in favor of disclosure." 450 F.2d at 674. The Court of Appeals also teaches in *Getman* that Exemption (6) is unique among the nine exemptions enumerated in § 552(b) in two major respects. First, it calls for the Court to exercise its discretion by balancing the interests of the parties, i. e. the right of the public to have access to governmental information against the right of personal privacy of affected individuals. 450 F.2d at 674. The Court stated in footnote 10:

"Any discretionary balancing of competing interests will necessarily be inconsistent with the purpose of the Act to give agencies, and courts as well, definitive guidelines in setting information policies . . . But Exemption (6), by its explicit language, calls for such balancing and must therefore be viewed as an exception to the general thrust of the Act. S.Rep., at 9, explains:

> 'The phrase "clearly unwarranted invasion of personal privacy" enunciates a policy that will involve a balancing of interests between the protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information. The application of this policy should lend itself particularly to those Government agencies where persons are required to submit vast amounts of personal data usually for limited purposes. * * *'

We note in passing that no other exemption specifically requires balancing. In view of the Act's basic purpose to limit discretion and encourage disclosure, we believe that Exemption (6) should be treated as unique, and that equitable discretion should not be imported into any of the other exemptions . . ." 450 F.2d at 674 n. 10.

Second, the Getman Court recognized that Exemption (6) is also unique in that the reasons of a plaintiff for requesting access to documents are relevant to the balancing process and must be taken into account. It stated:

"Although one of the purposes of the 1967 Freedom of Information Act was to limit agency discretion not to disclose by abandoning the former ground rule that a person requesting information show he was 'properly and directly concerned,' and by instead warranting disclosure to 'any person,' we find that this purpose is in unavoidable conflict with the explicit balancing requirement of

Exemption (6) . . . . *Since Exemption (6) necessarily requires the court to balance a public interest purpose for disclosure of personal information against the potential invasion of individual privacy, a court's decision to grant disclosure under Exemption (6) carries with it an implicit limitation that the information, once disclosed, be used only by the requesting party and for the public interest purpose upon which the balancing was based . . . .*" (emphasis supplied). 450 F.2d at 677 n. 24.

In the very recent case of Rural Housing Alliance v. U.S. Department of Agriculture et al., D.C.Cir., 498 F.2d 73, 77 (1974), the Court of Appeals stated: ". . . that in balancing interests the court should first determine if disclosure would constitute an invasion of privacy, and how severe an invasion. Second, the court should weigh the public interest purpose of those seeking disclosure, and whether other sources of information might suffice."

In the first prayer of the complaint and in his motion for summary judgment, plaintiff asks the Court to rule that the *Customs Declaration* forms be made available to him. He has also presented to the Court a form of order and judgment that is not limited to the disclosure of the names and addresses of the passengers but would also make available to him the complete Customs Declaration forms. This Court has concluded from the submissions of the parties that the disclosure of the highly personal and intimate details contained on the completed Customs Declaration forms for the purpose alleged by the plaintiff is totally unnecessary and would constitute a clearly unwarranted invasion of personal property. Having so concluded, the Court must now consider whether, under the circumstances of this case, the disclosure of the names and addresses only is foreclosed by Exemption (6).

In his appeal to the Commissioner, Bureau of Customs, dated August 7, 1973, plaintiff, through counsel, emphasized ". . . that the only information we want is the name and address of the passenger; we have no interest in obtaining any financial or commercial information."

The *Getman* Court, in ruling on the producibility of the Excelsior lists (names of persons eligible to vote in a representation dispute), stated ". . . in themselves a bare name and address give no information about an individual which is embarrassing"; and, after considering the purpose for which plaintiffs sought the lists, found that ". . . while recognizing that such disclosure does involve some invasion of privacy, . . . the invasion itself is to a very minimal degree." 450 F.2d at 675.

As distinguished from the finding of the Court of Appeals in *Getman*, this Court finds that the disclosure of the bare names and addresses sought herein by plaintiff will reveal that an individual was outside of the United States prior to a given date; the date of his return or initial entry to the United States; the general area of the world in which he had traveled; and the general area from which he came to the United States. Such information is confidential; may be embarrassing; and its disclosure would constitute a substantial invasion of privacy.

In the balancing process required by Exemption (6), the Court must consider also the reasons of the plaintiff for seeking access to the documents and weigh his public interest purpose. In his complaint plaintiff alleges that he ". . . . is seeking the names and addresses appearing on the Customs Declarations . . . in order to fulfill his obligations as representative of the class of all passengers who were charged unlawful fares pursuant to the violations of law alleged in . . ." a certain class action. It so happens, however, that this action is pending in the United States Court of Appeals, D.C. Circuit, on appeal from a judgment of the United States District Court dismissing the complaint. Assuming that the search for members of the class in a private lawsuit of this nature serves a public interest, if the Court of Appeals affirms the District Court's dismissal of the class action, plaintiff will have no reason to obtain the names and addresses of the passengers and no public interest purpose will then be served by such disclosure. On the other hand, if the Court of Appeals reverses the District Court and reinstates the Complaint, the plaintiff will have available to him other sources of obtaining the desired information. For example, he may, by use of the discovery rules of the Federal Rules of Civil Procedure, require the defendants to produce the names and addresses. Plaintiffs recognizes the availability of other sufficient sources of information. In footnote 5 of his Reply to Defendants' Motion To Dismiss Or In The Alternative For Summary Judgment, he states:

"In fact, some of the information contained on the Customs Declaration is available elsewhere. Civil Aeronautics Board Regulations require the airlines to maintain ticket coupons and reservation records. 14 C.F.R. § 249.13, lines 151(a) & 301. From these can be obtained the passenger's name, home and/or business telephone number, flight number and date, and often the passenger's address. Airlines also maintain flight manifests which contain the passenger's name and information about the flight. Finally, for those passengers who utilize credit cards, the receipt retained by the airline shows the passenger's name, information about the flight and the credit card number."

Attached to the above-mentioned Reply is the affidavit of plaintiff's counsel in which he states under oath that he has had lengthy discussions with counsel for Pan American, et al. in the above action and, as a result of those discussions and his own research, he has determined the availability of those other sources of information. In *Rural Housing Alliance, supra*, the Court of Appeals directs that in balancing interests ". . . the Court should weigh the public interest purpose of those seeking disclosure, and *whether other sources of information may suffice*." (Emphasis supplied).

In sum, this Court finds that disclosure of the names and addresses appearing on the Customs Declaration forms would constitute a substantial invasion of privacy; that such disclosure is unnecessary in this case; that protection of the individual from the potential invasion of privacy outweighs the public interest purpose for disclosure. Therefore, disclosure would constitute a "clearly unwarranted invasion of personal privacy."

Plaintiff's motion for summary judgment will be denied. Defendant's alternative motion for summary judgment will be granted.

WINE HOBBY USA, INC. v. UNITED STATES INTERNAL REVENUE SERVICE

Appeal of United States Bureau of Alcohol, Tobacco and Firearms.

No. 73-2072

UNITED STATES COURT OF APPEALS, THIRD CIRCUIT

SUBMITTED MAY 30, 1974—DECIDED AUGUST 19, 1974

Distributor of amateur wine-making equipment brought action under Freedom of Information Act to obtain names and addresses of persons filing form with Bureau of Alcohol, Tobacco and Firearms for purpose of being permitted to produce wine for use of their families without payment of tax. The United States District Court for the Eastern District of Pennsylvania, E. Mac Troutman, J., 363 F. Supp. 231 ordered that names and addresses be disclosed, and Government appealed. The Court of Appeals, Rosenn, Circuit Judge, held that information sought was within exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

Judgment reversed.

1. Records ⇐ 14

Purpose of Freedom of Information Act is to provide necessary machinery to assure the availability of government information necessary to an informed electorate by permitting access to official information shielded unnecessarily from public view and attempting to create judicially enforceable public right to secure such information from possibly unwilling official hands. 5 U.S.C.A. § 552.

2. Records ⇐ 14

Information, which, for advertising purposes, was sought pursuant to Freedom of Information Act by distributor of amateur wine-making equipment and which consisted of names and addresses of persons filing form with Bureau of Alcohol, Tobacco and Firearms for purpose of being permitted to produce wine for use of their families without payment of tax, was within exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C.A. §§ 552, 552(a)

(3), (b)(6); 26 U.S.C.A. (I.R.C. 1954) §§ 5041(a, d), 5042(a)(2), 5043 (a, b), 5661(a), 5687; Federal Alcohol Administration Act, §§ 3(b)(1), 7, 27 U.S.C.A. §§ 203(b)(1), 207.

3. Records ⇐ 14

Use of word "similar" within Freedom of Information Act exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" was not intended to narrow the exemption from disclosure and permit release of files which would otherwise be exempt because of resultant invasion of privacy. 5 U.S.C.A. §§ 552, 552(b)(6).

4. Records ⇐ 14

In determining whether information sought is within Freedom of Information Act exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," public interest purpose for disclosure of personal information must be balanced against potential invasion of individual privacy. 5 U.S.C.A. § 552(b)(6).

5. Records ⇐ 14

Disclosure of facts concerning family status of person, including fact that he is not living alone and that he exercises family control or responsibility in the household, constitutes an "invasion of personal privacy" within Freedom of Information Act exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C.A. § 552(b)(6).

Irving Jaffe, Acting Asst. Atty. Gen., Robert E. J. Curran, U.S. Atty., David M. Cohen, Meyer Rothwacks, Scott P. Crampton, Appellate Section, Tax Div., U.S. Dept. of Justice, Washington, D.C., for appellant.

James G. Watt, Butz, Hudders & Tallman, Allentown, Pa., for appellee.

Before KALODNER, ROSENN and HUNTER, Circuit Judges.

OPINION OF THE COURT

ROSENN, Circuit Judge.

This appeal requires us to consider the "invasion of privacy" exemption to the Freedom of Information Act, 5 U.S.C. § 552. Plaintiff, Wine Hobby USA, Inc. (Wine Hobby), a Pennsylvania corporation, brought suit to obtain the names and addresses of all persons who have registered with the United States Bureau of Alcohol, Tobacco and Firearms to produce wine for family use in the Mid-Atlantic region.[1] The district court ordered that the names and addresses be disclosed.[2] The Government appeals, contending

(1) that the material sought is exempt from compulsory disclosure under Exemption (6) to the Act, § 552(b)(6), which excludes from the Act's coverage "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," and

(2) alternatively, that the district court possesses equitable jurisdiction to decline to order disclosure in the circumstances of this case.

Under the Internal Revenue Code and the Federal Alcohol Administration Act, persons who produce wine are subject to certain permit, bonding, and tax requirements.[3] Criminal penalties are provided for noncompliance.[4] An exception to these requirements is provided by statute in the case of a "duly registered head of any family" who produces "for family use and not for sale an amount of wine not exceeding 200 gallons per annum."[5]

Pursuant to regulations,[6] registration under the stautory exception is effected

---

[1] The parties have stipulated in the district court that Wine Hobby has exhausted its administrative remedies.

[2] The district court's opinion is reported at 363 F. Supp. 231 (E.D.Pa. 1973). The court stayed its disclosure order pending this appeal.

[3] 26 U.S.C. §§ 5041 (a), (d); 5043 (a), (b); 27 U.S.C. § 203(b)(1).

[4] 26 U.S.C. §§ 5661(a), 5687; 27 U.S.C. § 207.

[5] 26 U.S.C. § 5042(a)(2).

[6] 26 C.F.R. §§ 240.540–543. The regulations provide that an individual is deemed to be the head of a family "only if he exercises family control or responsibility over one or more individuals closely connected with him by blood relationship, relationship by marriage, or by adoption, and who are living with him in one household." The exemption does not apply to, *inter alia*, "wine produced by a single person unless he is the head of a family" or "wine produced by a married man living apart from his family."

by filing Form 1541 with the Bureau of Alcohol, Tobacco and Firearms. Upon determination that the person is qualified, Form 1541 is stamped, one copy is returned to the registrant and the remaining copy is placed in the Bureau's files. Records of the Bureau indicate that in fiscal year 1973, 64,756 Forms 1541 were ary 1974, 41,585 Forms 1541 were on file, including 4,000 in the Mid-Atlantic region.

Wine Hobby is engaged in the business of selling and distributing amateur winemaking equipment and supplies to amateur winemakers through franchises, wholly owned retail stores, and by mail order. Wine Hobby has stipulated in the district court that its purpose in obtaining the names and addresses of the Form 1541 registrants is "to enable plaintiff to forward catalogues and other announcements to these persons regarding equipment and supplies that the plaintiff offers for sale." [7]

[1] We begin with the recogniton that the Freedom of Information Act, enacted to remedy the inadequacies of its predecessor, section 3 of the Administrative Procedure Act, 5 U.S.C. § 1002 (1964) :

> is broadly conceived. It seeks to permit access to official information long shielded unnecessarily from public view and attempts to create a judicially enforceable public right to secure such information from possibly unwilling official hands.

Environmental Protection Agency v. Mink, 410 U.S. 73, 80, 93 S.Ct. 827, 35 L.Ed.2d 119 (1973). The Act was intended to provide "the necessary machinery to assure the availability of Government information necessary to an informed electorate." [8] An integral part of the Act, however, is the nine enumerated exceptions. As the Senate Committee pointed out in its report :

> At the same time that a broad philosophy of "freedom of information" is enacted into law, it is necessary to protect certain equally important rights of privacy with respect to certain information in Government files, such as medical and personnel records. It is also necessary for the very operation of our Government to allow it to keep confidential certain material, such as the investigatory files of the Fedreal Bureau of Investigation.

Senate Report No. 813, 89th Cong., 1st Sess. 3 (1965) (hereinafter "S. Rep.").

[2] The Government relies on Exemption (6) as the basis for refusing to supply the information requested by Wine Hobby. The district court reluctantly concluded that despite the potential for abuse, the names and addresses sought here were not subject to this exemption as an invasion of privacy. The court also held that it had no power to exercise its equitable discretion to withhold and no alternative but to grant the request. We hold that the names and addresses sought are within the exemption and we therefore reverse.

To qualify under Exemption (6), the requested information must consist of "personnel, medical or similar files," and the disclosure of the material must constitute a "clealy unwarranted invasion of personal privacy."

We believe that the list of names and addresses is a "file" within the meaning of Exemption (6). A broad interpretation of the statutory term to include names and addresses is necessary to avoid a denial of statutory protection in a case where release of requested materials would result in a clearly unwarranted invasion of personal privacy. Since the thrust of the exemption is to avoid unwarranted invasions of privacy, the term "files" should not be given an interpretation that would often preclude inquiry into this more crucial question.[9]

[3] Furthermore, we believe the list of names and addresses is a file "similar" to the personnel and medical files specifically referred to in the exemption. The common denominator in "personnel and medical and similar files" is the personal quality of information in the file, the disclosure of which may constitute a clealy unwarranted invasion of personal privacy. We do not believe that the use of the term "similar" was intended to narrow the exemption from disclosure and permit the release of files which would otherwise be exempt because of the resultant invasion of privacy.

---

[7] Wine Hobby has declined to participate in this appeal, either in filing briefs or participating in oral argument.

[8] H. Rep. No. 1497, 89th Cong. 2d Sess. (1966), reproduced, 1966 U.S. Code, Cong. & Admin. News, pp. 2418–2429 (hereinafter "H. Rep.").

[9] For example, were purchasers of contraceptives required to register with the Government, and were a plaintiff to request disclosure of the names and addresses of such registrants, a narrow construction of "files" would require disclosure by preventing inquiry into the invasion of privacy which would result from disclosure.

We now turn to the Government's contention that disclosure of the names and addresses to Wine Hobby would result in a "clearly unwarranted invasion of personal privacy." Because of an apparent conflict in the circuits,[10] we must first consider whether the statutory language, which clearly demands an examination of the invasion of privacy, also requires inquiry into the interest in disclosure.

[4] Our examination of the statute and its legislative history leads us to conclude, in the language of the District of Columbia Circuit, that "Exemption (6) necessarily requires the court to balance a public interest purpose for disclosure of personal information against the potential invasion of individual privacy." Getman v. N.L.R.B., 450 F.2d at 677 n. 24 (1971).[11] On its face, the statute, by the use of term "unwarranted," compels a balancing of interest. The interpretation, moreover, is supported by the legislative history.[12]

We disagree with the view of the Fourth Circuit that the language of § 552 (a) (3) precludes a balancing of interests to determine the application of Exemption (6).[13] That paragraph which amended a provision of section 3 of the Administrative Procedure Act which required that the plaintiff be "properly and directly concerned," authorizes release of information to "any person." The Fourth Circuit apparently construed the amendment to prevent an inquiry into the purpose asserted by an individual plaintiff. Significantly, however, the paragraph applies only to matters not within any of the exemptions enumerated in § 552(b). Thus it is only *non-exempt* material that must be made available to "any person." [14] We see nothing in § 552(a) (3) therefore that precludes balancing to determine whether particular information is within a statutory *exemption.*

[5] To apply the balancing test to the facts of this case we must determine whether release of the names and addresses would constitute an invasion of personal privacy and, if so, balance the seriousness of that invasion with the purpose asserted for release. Getman v. N.L.R.B., *supra.* Turning to the first consideration, we conclude that disclosure would involve an invasion of privacy. As the Government points out in its brief, there are few things which pertain to an individual in which his privacy has traditionally been more respected than his own home. Mr. Chief Justice Burger recently stated:

> The ancient concept that "a man's home is his castle" into which "not even the king may enter" has lost none of its vitality. . . .

Rowan v. United States Post Office Dept., 397 U.S. 728, 737, 90 S.Ct. 1484, 1491, 25 L.Ed.2d 736 (1970). Disclosure of the requested lists would involve a release of each registrant's home address, information that the individual may fervently wish to remain confidential or only selectively released.[15] One consequence of this

---

[10] Compare Getman v. N.L.R.B., 146 U.S. App. D.C. 209, 450 F.2d 670 (1971), and Rose v. Dept. of the Air Force, 495 F.2d 261 (2d Cir., 1974), with Robles v. Environmental Protection Agency, 484 F.2d 843 (4th Cir. 1973). *See also* Note, Invasion of Privacy and the Freedom of Information Act: Getman v. N.L.R.B., 40 Geo. Wash. L. Rev. 527 (1972).

[11] In *Getman*, the court considered the application of Exemption (6) to a request by two labor law professors for the lists of names and home addresses of employees eligible to vote in representation elections. The professors were engaged in a study of N.L.R.B. representation election rules and intended to use the employee lists to facilitate the scheduling of interviews with affected employees. The court held the employee lists disclosable, finding that disclosure for the purpose of the professors' study was "if anything . . . clearly warranted."

[12] The Senate Report provides (at 9):

> The phrase "clearly unwarranted invasion of personal privacy" enunciates a policy *that will involve a balancing of interests* between the protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information. The application of this policy should lend itself particularly to those Government agencies where persons are required to submit vast amounts of personal data usually for limited purposes. . . . [Emphasis supplied.]

[13] Robles v. Environmental Protection Agency, 484 F. 2d 843 (4th Cir. 1973).

In *Robles*, plaintiffs sought the names and addresses of persons who occupied buildings which had been monitored by the E.P.A. for radiation levels and possible radioactive emissions. The court held Exemption (6) inapplicable and ordered disclosure.

[14] The Senate Report provides (at 5–6):

> [The proposed Act] eliminates the test of who shall have the right to different information. For the great majority of different records, the public as a whole has a right to know what its Government is doing. There is, of course, a certain need for confidentiality in some aspects of Government operations and these are protected specifically: but *outside these limited areas, all citizens have a right to know.* [Emphasis supplied.]

[15] That society recognizes the individual's interest in keeping his address private is indicated in such practices as non-listing of telephone numbers and the renting of post office boxes.

disclosure is that a registrant will be subjected to unsolicited and possibly unwanted mail from Wine Hobby and perhaps offensive mail from others.[16] Moreover, information concerning personal activities within the home, namely wine-making, is revealed by disclosure. Similarly, dislosure reveals information concerning the family status of the registrant, including the fact that he is not living alone and that he exercises family control or responsibility in the household. Disclosure of these facts concerning the home and private activities within it constitutes an "invasion of personal privacy."

We must now balance the seriousness of this invasion of privacy against the public interest purpose asserted by the plaintiff. As noted, the sole purpose for which Wine Hobby has stipulated that it seeks the information is for private commercial exploitation. Wine Hobby advanced no direct or indirect public interest purpose in disclosure of these lists and indeed, we can conceive of none.[17] The disclosure of names of potential customers for commercial business is wholly unrelated to the purposes behind the Freedom of Information Act and was never contemplated by Congress in enacting the Act. In light of this failure by Wine Hobby to assert a public interest purpose for disclosure, we conclude that the invasion of privacy caused by disclosure would be "clearly unwarranted," even though the invasion of privacy in this case is not as serious as that considered by the court in other cases, *see, e.g.*, Rose v. Dept. of the Air Force, 495 F.2d 261 (2d Cir. 1974).[18] On balance, therefore, we believe that the list of names and addresses of the Form 1541 registrants is exempted from disclosure under § 552 (b) (6) in the circumstances of this case.

Because we believe that the information requested by Wine Hobby is exempted from disclosure under a specific statutory exemption, we need not reach the question of whether, were the material not specifically exempted, the district court possesses equitable jurisdiction to decline to order disclosure.

The judgment of the district court will be reversed.

WINE HOBBY, USA, INC. *v.* UNITED STATES BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

Civ. A. No. 72-1629

UNITED STATES DISTRICT COURT, E. D. PENNSYLVANIA, SEPTEMBER 10, 1973

Distributor of wine-making equipment brought action under Freedom of Information Act to obtain names and addresses of persons who, for purposes of being permitted to produce wine for use of their families without payment of tax, filed form in region of Bureau of Alcohol, Tobacco and Firearms. On parties' motions for summary judgment, the District Court, Troutman, J., held that information sought was not subject to statutory exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

Plaintiff's motion granted; defendant's motion denied.

1. Records ⇐ 14

Needs of party seeking relief under Freedom of Information Act, including fact that plaintiff is motivated by personal economic gain, may not be considered. 5 U.S.C.A. § 552.

---

[16] As Chief Justice Burger stated in *Rowan, supra:*

[T]he right of every person "to be let alone" must be placed in the scales with the right of others to communicate.

In today's complex society we are inescapably captive audiences for many purposes, but a sufficient measure of individual autonomy must survive to permit every householder to exercise control over unwanted mail. . . . It places no strain on the doctrine of judicial notice to observe that whether measured by pieces or pounds, Everyman's mail today is made up overwhelmingly of material he did not seek from persons he does not know. And all too often it is matter he finds offensive.

397 U.S. 728, 736, 90 S. Ct. 1484, 1490, 25 L. Ed. 2d 736 (1970).

In *Rowan*, the Court upheld the constitutionality of a statute that authorized the Postmaster General, at the request of an addressee who objected to advertisements as "erotically arousing or sexually provocative," to direct a sender to remove the addressee's name from his mailing list.

[17] Denial of the lists, moreover, would impose no private hardship as Wine Hobby may accomplish its stated purpose, advertising, through the general media without specific mailings.

[18] The court in *Rose* refused to permit disclosure of case summaries of military honor code adjudications if such disclosure would reveal the identity of the cadets involved.

2. Records ⊜ 14

Unless information sought under Freedom of Information Act falls squarely within a statutory exemption, request for information must be granted, and court has no right to exercise equitable discretion. 5 U.S.C.A. § 552.

3. Records ⊜ 14

Access to material under Freedom of Information Act is not limited to those persons with particular reason for seeking disclosure; instead, material is available to any person. 5 U.S.C.A. § 552.

4. Records ⊜ 14

Information sought under Freedom of Information Act by corporation, which was distributor of wine-making equipment, as to names and addresses of persons who, for purposes of being permitted to produce wine for use of their families without payment of tax, filed form in region of Bureau of Alcohol, Tobacco and Firearms, was not subject to statutory exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C.A. §§ 552, 552(a)(2), (b), (b)(6).

James G. Watt, Allentown, Pa., for plaintiff.
Carmen Nasuti, Asst. U. S. Atty., Philadelphi,a Pa., for defendant.

MEMORANDUM AND ORDER

TROUTMAN, District Judge.

This is an action brought by the plaintiff under the Freedom of Information Act (the Act), 5 U.S.C. § 552, to obtain the names and addresses of all persons filing United States Bureau of Alcohol, Tobacco and Firearms Form 1541 (registration for production of wine for family use) in the Mid-Atlantic region of the United States.

Bureau of Alcohol, Tobacco and Firearms regulations 26 CFR §§ 240, 540–543, provide that the head of a family may, without payment of tax, produce 200 gallons of wine a year for the use of his family, and not for sale, if he registers to do so by filing Bureau of Alcohol, Tobacco and Firearms Form 1541. (Stip., Par. 3) After a determination is made that the person is qualified for an exemption, Form 1541 is stamped and one copy is returned to the registrant and the remaining copy placed in a file by the Bureau.

Wine Hobby, U.S.A., Inc. is a Pennsylvania corporation with its principal office in Allentown, Pennsylvania. It is engaged in the business of importing wine-making equipment and supplies from abroad as well as purchasing similar items in the United States and selling and distributing such items through retail stores, through franchises and by mail order to amateur winemakers. (Stip., Par. 2) In order to solicit business, Wine Hobby, U.S.A., Inc. mails out catalogs and notices of new items they offer for sale.

Wine Hobby, U.S.A., Inc. seeks the names and addresses of all persons filing Form 1541 in the Mid-Atlantic region of the Bureau of Alcohol, Tobacco, and Firearms in order that they may forward catalogs and other announcements regarding equipment and supplies that plaintiff has for sale. (Stip., Par. 4)

The Freedom of Information Act, 5 U.S.C. § 552, provides that each governmental agency shall make available to the public the information therein specified, including its organizational set-up, the methods by which it functions, its rules and procedure, its opinions, statements of policy, interpretations, manuals and instructions. Significantly, as regards the above information, not involved in this case, the act provides, *inter alia*, "to the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details * * *". 5 U.S.C. § 552(a)(2).

Section 552(b) provides:

"(b) This section does not apply to matters that are—

(1) specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of, an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells."

The defendant contends that the names and addresses of those who have obtained a Form 1541 are protected by sub-paragraph (6), *supra*, as a "clearly unwarranted invasion of personal privacy".

At the very threshold, we note, as already indicated, that any such agency "may delete identifying details" under Section 552(a)(2) "to prevent a clearly unwarranted invasion of personal privacy". Here, however, it is "identifying" details, specifically names and addresses, which the plaintiff seeks. The defendant, therefore, understandably argues that the plaintiff is not entitled to the information sought and relies specifically upon sub-section (6), relating as it does to "invasion of personal privacy".

In Consumers Union of United States, Inc. v. Veterans Administration, 301 F. Supp. 796 (S.D.N.Y. 1969), the Court delineated the purposes of the Act as follows:

"* * * The purpose of the Act, seen in the statutory language and the legislative history, was to reverse the self-protective attitude of the agencies under which they had found that the public interest required, for example, that the names of unsuccessful contract bidders be kept from the public. The Act made disclosure the general rule and permitted only information specifically exempted to be withheld; it required the agency to carry the burden of sustaining its decision to withhold information in a de novo equity proceeding in a district court. Disclosure is thus the guiding star for this court in construing the Act. * * *" 301 F. Supp. at 799, 800.

Interestingly, the Court further noted as follows:

"Even though the records sought are not exempt, the court is not bound under the Act to automatically order their disclosure. In exercising the equity jurisdiction conferred by the Act, it must, according to traditional equity principles, weigh the effects of disclosure and non-disclosure and determine the best course to follow at the present time. In an action under the Freedom of Information Act, which shifts the burden of proof to the defendant, the balance of the equities is presumptively on the side of disclosure. The rule that will be followed, therefore, is this: where agency records are not exempted from disclosure by the Freedom of Information Act, a court *must* order their disclosure unless the agency proves that disclosure will result in significantly greater harm than good. Because the Act was intended to benefit the public generally, it is primarily the effects on the public rather than on the person seeking the records that must be weighed." (Emphasis ours) 301 F. Supp. at 806.

Again referring to the broad purposes of the Act, the Court in Bristol-Myers Company v. Federal Trade Commission et al., 138 U.S. App. D.C. 22, 424 F. 2d 935 (1970) said as follows:

"The legislative history establishes that the primary purpose of the Freedom of Information Act was to increase the citizen's access to government records. Before 1967, the Administrative Procedure Act contained a Public Information section 'full of loopholes which allow[ed] agencies to deny legitimate information to the public'. When Congress acted to close those loopholes, it clearly intended to avoid creating new ones. * * *"

The noble purpose of the Act was specifically alluded to in American Mail Line, Ltd. et al. v. J. W. Gulick et al., 133 U.S. App. D.C. 382, 411 F. 2d 696 (1969), where the Court stated:

"The Freedom of Information Act was promulgated in 1966 (80 Stat. 250) with a stipulation that it would not take effect until July 4, 1967 (81 Stat. 54), and it is now codified in 5 U.S.C. § 522 (Supp. III, 1965–1967). An exploration of the legislative history behind this enactment reveals that the premier purpose of the Act was to elucidate the availability of Government records and actions to the American citizen. In addition, Congress sought to eliminate much of

the vagueness of the old law (section three of the Administrative Procedure Act of 1946, 60 Stat. 238). The Senate Report characterized the purpose of the Act as follows (S. Rep. No. 813 at 2-3):

"Knowledge will forever govern ignorance, and a people who mean to be their own governors, must arm themselves with the power knowledge gives. A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both. With this noble purpose we wholheartedly agree. * * *" (411 F. 2d at 699.)

More recently, in Environmental Protection Agency et al. v. Mink et al., 410 U.S. 73, 93 S. Ct. 827, 35 L. Ed. 2d 119 (1973), Mr. Justice Douglas, dissenting, said as follows:

"* * * We should remember the words of Madison: 'A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power knowledge gives'." 410 U.S. at 110, 93 S. Ct. at 847.

[1] In Soucie v. David, 145 U.S. App. D.C. 144, 448 F. 2d 1067 (1971), the Court, in construing the Act, said as follows:

"* * * The Act rejects the usual principle of deference to administrative determinations by requiring a trial 'de novo' in the district court. By directing disclosure to *any person, the Act precludes consideration of the interest of the party seeking relief.* Most significantly, the Act expressly limits the grounds for non-disclosure to those *specified in the exemption.* * * *" (Emphasis ours.)

Thus, we are precluded from considering the needs of the party seeking relief. The fact that plaintiff is motivated by personal economic gain in the promotion of its product is considered by the Court to be of no significance and we are precluded from its consideration.

Of equal significance and importance was the next succeeding comment of the Court as follows:

"* * * Through the general disclosure requirement and specific exemptions, *the Act thus strikes a balance among factors* which would ordinarily be deemed relevant to the exercise of equitable discretion, i.e., the public interest in freedom of information and countervailing public and private interests in secrecy. *Since judicial use of traditional equitable principles to prevent disclosure would upset this legislative resolution of conflicting interests, we are persuaded that Congress did not intend to confer on district courts a general power to deny relief on equitable grounds apart from the exemptions in the Act itself.* * * *" 448 F. 2d at 1077. (Emphasis ours)

Here we are instructed that the Act itself strikes the balancing factors and that this Court is, therefore, precluded from exercising its historic equitable power.

In Getman et al. v. National Labor Relations Board, 146 U.S. App. D.C. 209, 450 F.2d 670 (1971) names and addresses of employees eligible to vote in certain elections before the National Labor Relations Board were sought by certain professors of labor law, ostensibly interested in studying the procedures of the Board with a view to the improvement thereof and, thus, an improvement in governmental operations. The Court stated:

"* * * We hold further that a District Court has no equitable jurisdiction to permit withholding of information which does not fall within one of the exemptions of the Act. * * *" 450 F.2d at 672.

Considering specifically Exemption (6) with which we are here concerned, the Court further stated:

"Although Exemption (6) differs from Exemptions (4) and (7) in that it covers information similar in some respect to the kind being sought in this case, we agree with the District Court that the Board has not met the burden of proof required to justify a refusal to disclose under this part of the Act. Exemption (6) applies to 'personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy'. Assuming that the Excelsior lists may be characterized as 'personnel and medical files and similar files', it is still only a disclosure constituting a 'clearly unwarranted invasion of personal privacy' that falls within the scope of Exemption (6). Exemption (6) requires a court reviewing the matter de novo to balance the right of privacy of affected individuals against the right of the public to be informed; and the statutory language 'clearly unwarranted' instructs the court to tilt the balance in favor of disclosure.

"In carrying out the balancing of interests required by Exemption (6), our first inquiry is whether disclosure of the names and addresses of employees constitutes an invasion of privacy and, if so, how serious an invasion. We find that, although a limited number of employees will suffer an invasion of privacy in losing their anonymity and in being asked over the telephone if they would be willing to be interviewed in connection with the voting study, the loss of privacy resulting from this particular disclosure should be characterized as relatively minor. * * * The giving of names and addresses is a very much lower degree of disclosure; in themselves a bare name and address give no information about an individual which is embarrassing. In the conduct of appellees' study, any disclosure of information more personal than a name and address is wholly consensual and within the control of the employee. * * * Thus assuming arguendo that the disclosure of Excelsior lists constitutes disclosure of a 'file' within the meaning of Exemption (6), and while recognizing that such disclosure does involve some invasion of privacy, we find that the invasion itself is to a very minimal degree.

"In determining whether this relatively minor invasion of privacy is 'clearly unwarranted', we must also weigh the public interest purpose of appellees' NLRB voting study, the quality of the study itself, and the possibility that appellees could pursue their study without the Excelsior lists. * * *

"* * * The public interest need for such an empirical investigation into the assumptions underlying the Board's regulation of campaign tactics has for some time been recognized by labor law scholars. This particular study has been reviewed and supported by virtually every major scholar in the labor law field. The record is also replete with testimonials from leading management and union representatives and Government officials. Appellees' research has also been approved by the prestigious National Science Foundation, which has awarded appellees the largest grant ever made available for law related reserch."

Thus, under Exemption (6), the Court indulged in a balance of equities, concluding that the invasion of privacy was minimal.

Turning then to the question whether the courts have equitable discretion to permit withholding of information which does *not* fall within one of the specific exemptions, the Court stated:

"Having found that nondisclosure of the Excelsior lists is not warranted under Exemption (4), (6) or (7), we must still resolve the *question whether the courts has equitable discretion to permit withholding of information which does not fall within one of the specific exemptions to the Act.* The District Court in this case held that, [a]ssuming that [a District Court], in an action under the Freedom of Information Act, may deny disclosure on grounds other than those set out in the specific exemptions to the Act, the burden of justifying non-disclosure must still rest upon the agency. I find that the Board has not met that burden.' We do not need to reach the balancing issue decided by the District Court because we agree with the dicta of the panel in Soucie v. David, 145 U.S.App.D.C. 144, 448 F.2d 1067 (decided April 13, 1971), and with the Fourth Circuit's decision in Wellford v. Hardin, 444 F.2d 21 (1971), that a District Court has no equitable jurisdiction to deny disclosure on grounds other than those laid out under one of the Act's enumerated exemptions." 450 F.2d at 677 and 678. (Emphasis ours)

In support of its conclusion, the Court stated:

"* * * The basic purpose of the amendment which has become popularly known as the Freedom of Information Act, was to guarantee public access to Government information by converting a 'withholding' statute to a 'disclosure' statute and by mandating full public access to Government information, subject to a limited number of clearly drawn exemptions.

"The question whether the courts retain equitable discretion under the Act is settled for us by the express language of the Act, aided by the gloss from the Senate report. Section 552(c) states: 'This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. * * *' " 450 F.2d at 679.

[2, 3] Thus, unless the information falls squarely within Exemption (6), we have no right to the exercise of discretion and no alternative but to grant the plaintiff's request. Access to material under the Freedom of Information Act is not limited to those persons with particular reason for seeking disclosure; instead material is available to "any person". Hawkes v. Internal Revenue Service, 467 F.2d 787 (6th Cir. 1972).

[4] The defendant relies, by analogy, upon N.A.A.C.P. v. Alabama, 357 U.S. 449, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958) holding that the State of Alabama could

not force the disclosure of the names and addresses of members of an organization associated together for the advancement of beliefs, ideals and ideas assured by the Due Process Clause of the Fourteenth Amendment. The decision was squarely predicated upon the possibility of economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility adversely affecting the ability of the association and its members to pursue their collective efforts. It clearly has no application here. Likewise see Griswold v. Connecticut, 381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965).

In Legal Aid Society of Alameda County et al. v. Shultz, 349 F.Supp. 771, N.D.Cal.1972), the Court specifically directed the disclosure of "a list of the names of all federal nonconstruction contractors assigned to the Department of the Treasury for compliance purposes under Executive Order No. 11246 that are subject to the requirements of 41 C.F.R. § 60–1.40 and that have an establishment located in Alameda County, California". The Court noted its lack of equitable discretion:

"* * * it is now well settled that because of the specific command of § 552(c), discussed above, the courts have no discretion to refuse to order disclosure on equitable principles. See Getman v. NLRB, 146 U.S.App.D.C. 209, 450 F.2d 670, 677–680 (1971); Soucie v. David, 145 U.S.App.D.C. 144, 448 F.2d 1067, 1076–1077 (1971)." 349 F.Supp. at 776.

Thus, careful review of applicable authorities and precedents discloses that the names and addresses here sought are not subject to Exemption (6) as an invasion of privacy. This is not to suggest that we agree with the conclusion, under the facts here involved, or find that such result was in fact the congressional intent. Rather, we think Circuit Judge MacKinnon, in the concurring opinion in Getman v. National Labor Relations Board, *supra*, correctly stated as follows:

"The extremely broad sweep of the Freedom of Information Act, with its narrow exemptions, makes it *mandatory* in my opinion—if we are to follow the directions of Congress—to direct the National Labor Relations Board to furnish appellees with the names and addresses of employees as requested. * * *

"My principal concern is for the future. We are here following the dictates of Congress and are making information available for a use that may interfere with the proper functioning of government. This use may have its beneficial effects also, but before the good is harvested considerable turmoil and disruption may result. And this decision is only the beginning. *We may expect similar wholesale demands for lists of names and addresses from other persons, not for what they may disclose about the functioning of government, but for their collateral ability to aid the person requesting such information.*

* * * * * * *

"*It seems to me that furnishing bare lists of names and addresses of various groups of persons in various Government files is not the sort of disclosure that Congress basically had in mind in enacting the Freedom of Information Act. Yet in my opinion, the Act as it presently exists practically requires the disclosure of such lists on demand. One need not elaborate on the various abuses that could result if lists of people as classified by the Government for particular purposes became available practically on demand in wholesale lots. If this situation is to be corrected, it will require an amendment to the Act.*" (Emphasis ours) 449 F.2d at 680, 681.

We agree with Judge MacKinnon. We suggest that the lanuage used in Section (a)(2), namely,

"* * * to the extent required to prevent a clearly unwarranted invasion of personal privacy, *an agency may delete identifying details* when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction", indicates a congressional intent to delete or eliminate precisely all "identifying details" here sought and it is unfortunate that such language was not included in sub-section (b) as regards exemptions. If such language indicates an intent by Congress to eliminate precisely what is occurring here, it is unfortunate that the courts have not, in recognition of Judge MacKinnon's prophetic language, given this Court the equitable discretion required to properly deal with the situation. It must come as a surprise to the head of a family, procuring less than two hundred gallons of homemade wine per year for his own use, as procuring Form 1541 as he is legally obliged to do, to find that his name has become a part of a vast list of names released by the Government for purposes of commercial exploitation. We hasten to add that in this instance, as stated by

reputable and dependable counsel for the plaintiff, there is no reason to suspect that the list will be improperly used or that the subject will receive anything more than an advertisement in which indeed he may have considerable personal interest and for which he may be grateful. That happy circumstance existing in this case, under the facts presented to us, does not eliminate the unhappy situation which may follow in the next instance when the Government is thus forced to disclose a name and address. In reaching our conclusion, we hope that the observations just made are the result of unwarranted and unjustified speculation. However, common sense compels us to the conclusion reached by Judge MacKinnon as regards the potential abuses that may result from this and like decisions.

We will grant the plaintiff's motion for summary judgment and deny the defendant's motion for summary judgment.

RURAL HOUSING ALLIANCE

v.

UNITED STATES DEPARTMENT OF AGRICULTURE ET AL., APPELLANTS

No. 73-1771

UNITED STATES COURT OF APPEALS, DISTRICT OF COLUMBIA CIRCUIT

ARGUED DECEMBER 5, 1973—DECIDED JUNE 3, 1974
REHEARING DENIED JULY 3, 1974—REHEARING DENIED SEPTEMBER 24, 1974, SEE 502 F.2d 1179

Action by private organization to obtain disclosure of report of investigation by Department of Agriculture of governmental housing discrimination. The United States District Court for the District of Columbia, John Lewis Smith, Jr., J., granted plaintiff's motion for summary judgment and the Secretary of Agriculture appealed. The Court of Appeals, Wilkey, Circuit Judge, remanded case for determination of factual issues as to whether report involved sufficiently intimate details concerning individuals to be exempt from disclosure under provision of Freedom of Information Act exempting personnel and medical files and similar files, the disclosure of which would constitute unwarranted invasion of privacy, whether the information in the report was exempt from disclosure as confidential or privileged financial information and whether the report was exempt as an investigatory file compiled for law enforcement purposes.

Reversed and remanded.

1. Records ⇐ 14

Exemption from disclosure under Freedom of Information Act of personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, was designed to protect individuals from public disclosure of intimate details of their lives, and exemption is not limited to Veterans Administration or Social Security files, but rather is phrased broadly to protect individuals from a wide range of embarrassing disclosures. 5 U.S.C.A. § 552(a)(2), (b), (b)(4, 6, 7).

2. Records ⇐ 14

Where report of investigation by Department of Agriculture of governmental housing discrimination contained information regarding marital status, legitimacy of children, identity of fathers of children, medical condition, welfare payments, alcoholic consumption, family fights and reputation, the report involved sufficiently intimate details to be "similar file" within Freedom of Information Act exempting from disclosure personnel and medical files and similar files, the disclosure of which would constitute clearly unwarranted invasion of personal privacy. 5 U.S.C.A. § 552(a)(2), (b), (b)(4, 6, 7).

3. Records ⇐ 14

In balancing interests under Freedom of Information Act, court should first determine if disclosure would constitute an invasion of privacy and how severe an invasion and secondly court should weigh public interest purpose of those seeking disclosure and whether other sources of information might suffice. 5 U.S.C.A. § 552(a)(2), (b), (b)(4, 6, 7).

4. Records ⇐ 14

In determining whether private organization was entitled to obtain disclosure of report of investigation by Department of Agriculture of governmental housing discrimination, district court should determine nature and extent of invasion of individuals' privacy, consider whether deletions previously ordered were sufficient to protect privacy of individuals, consider public interest purpose of private organization and whether it could be achieved without the material or any alternate available sources of information and the balancing of factors must thereafter be made. 5 U.S.C.A. § 552(a)(2), (b), (b)(4, 6, 7).

5. Records ⇐ 14

Exemption from Freedom of Information Act of trade secrets and commercial or privileged or confidential financial information obtained from a person is primarily a trade secrets exemption, but it also protects individuals from disclosure of financial information which is privileged or confidential. 5 U.S.C.A. § 552(b)(4).

6. Records ⇐ 14

Bare claim by interested governmental agency of confidentiality of financial information is not sufficient to preclude disclosure under Freedom of Information Act. 5 U.S.C.A. § 552(b)(4).

7. Records ⇐ 14

With respect to report of investigation by Department of Agriculture of governmental housing discrimination, information relating to loan applications was within ambit of Freedom of Information Act exemption applicable to privileged or confidential financial information for purposes of determining whether private organization was entitled to obtain disclosure of the report. 5 U.S.C.A. § 552(b)(4).

8. Records ⇐ 14

For provision of Freedom of Information Act exempting from disclosure investigatory files compiled for law enforcement purposes to be applicable, government need not show imminent adjudicatory proceedings or concrete prospect of enforcement proceedings, but is required to show only that files were compiled for adjudication or enforcement purposes. 5 U.S.C.A. § 552(b)(7)

9. Records ⇐ 14

If purpose of investigation by Department of Agriculture of governmental housing discrimination was to consider an action equivalent to those which government brings against private parties, thus demonstrating that "law enforcement purpose" was not customary surveillance of performance of duties by government employees, but inquiry as to an identifiable possible violation of law, then such inquiry would have been "for law enforcement purposes" within provision of Freedom of Information Act exempting from disclosure investigatory files compiled for law enforcement purposes, whether the individual were private citizen or government employee. 5 U.S.C.A. § 552(b)(7).

10. Records ⇐ 14

In determining whether government investigation was an inquiry as to an identifiable possible violation of law, and thus "for law enforcement purposes" within provision of Freedom of Information Law exempting from disclosure investigatory files filed for law enforcement purposes, court must be wary of self-serving declarations of any agency and it must be clear to court that more than ephemeral possibilities of enforcement were anticipated by agency in undertaking the investigation. 5 U.S.C.A. § 552(b)(7).

11. Records ⇐ 14

If investigatory file is compiled by government agency for purpose of determining whether a law enforcement proceeding should be brought in same manner as against a private citizen and against whom, then, whether agency concludes that proceedings are necessary or not, it may utilize provision of Freedom of Information Act exempting from disclosure investigatory files compiled for law enforcement purposes to protect its investigatory process and sources. 5 U.S.C.A. § 552(b)(7).

David M. Cohen, Atty., Dept. of Justice, of the bar of the Supreme Court of Ill., pro hac vice by special leave of court with whom Irving Jaffe, Acting Asst.

Atty. Gen., Harold H. Titus, Jr., U.S. Atty., and Leonard Schaitman, Atty., Dept. of Justice, were on the brief, for appellants. Harold H. Titus, Jr., U.S. Atty., John A. Terry and Derek I. Meier, Asst. U.S. Attys., also entered appearances for appellants.

Victor H. Kramer, Washington, D.C., with whom Richard B. Wolf, Washington, D.C., was on the brief, for appellee.

Before BAZELON, Chief Judge, and ROBB and WILKEY, Circuit Judges.

WILKEY, Circuit Judge:

We have before us once again the question of the proper interpretation of several exemptions from disclosure under the Freedom of Information Act [FOIA].[1] At issue here is a report of a U.S. Department of Agriculture investigation of governmental housing discrimination in Florida, withheld from disclosure on the basis of exemptions 4, 5, 6, and 7. The District Court granted the plaintiff Rural Housing Alliance [RHA] motion for summary judgment after *in camera* inspection holding that the report was not within any exemption.[2] We find the District Court applied incorrect legal standards in evaluating the applicability of the exemptions, hence reverse the judgment and remand for consideration consistent with this opinion.

I. THE NATURE OF THE GOVERNMENT REPORT

The USDA report and the investigation which spawned it were stimulated by an RHA pamphlet, "Studies in Bad Housing in America—Abuse of Power." Utilizing a method of case-history documentation, this RHA tract charged the Farmers Home Administration [FmHA] staff with racial and national origin discrimination in arranging government loans under the Rural Housing Program in two counties in Florida.[3] The Office of Equal Opportunity of the USDA requested an investigation by the Department's Office of Inspector General [OIG]. After investigation, the OIG concluded in a 150-page report that there was no substantial evidence indicating discrimination.

RHA's request for a copy of the investigation report was denied. Instead, OIG made public the "Investigation Summary" and "Statistical Data" sections of the report. Citing exemptions 4, 5, 6, and 7 of FOIA as valid justification for keeping the remainder confidential, the Government did not release the remainder of the report because the Government felt that its form—detailed and intimate case histories of specified, named persons[4]—was inappropriate for disclosure. The Government did indicate that the material would be disclosed to RHA if it produced written authorization for release from the particular individual involved in any section.[5] Rather than obtain such releases, RHA brought this FOIA suit.

The District Court, in considering RHA's motion for summary judgment, found that the report as a whole was not exempt from disclosure. However, the court recognized that there might be a need to delete details which would permit identification of the individuals involved. Consequently, the court ordered deletion of the names of applicants for loans, the names of those who complained to their Congressmen, those who were interviewed, attorneys, etc. Deletion of geographical references, applications for loans, and affidavits of applicants was likewise ordered.[6]

---

[1] 5 U.S.C. § 552 (1970).

[2] The District Court ordered deletions of identifying details to be made; these are discussed at p. 76 *infra*.

[3] The two counties are Martin and Palm Beach Counties.

[4] Inspector General Kossack's affidavit of 29 January 1973 stated that

> The report includes intimate details and information given by and with respect to borrowers and applicants for loans regarding the marital status of such borrowers and applicants, the number and the legitimacy of their children and grandchildren, and the identity of the fathers of their children; information as to their medical condition and history, including statements as to surgery and the possibility of future pregnancies; information as to their occupations and work history and the amounts and sources of their annual income, including the amount of welfare payments received; information as to their ownership of property; information as to their habits with respect to the consumption of alcoholic beverages; information as to family fights which had occurred; information from their employers as to their reliability as employees; information as to their reputation in the community; information as to the risks involved in extending credit to them; and other information of a clearly personal and confidential nature. Appendix at 43–44.

[5] Brief for Appellant at 7.

[6] District Court Order of 9 May 1973, in Appendix at 69–70.

USDA then filed a motion to clarify or amend the court's order. In support of the motion, USDA submitted an affidavit of the Inspector General, Nathaniel Kossack, explaining the Government's fear that the court order as framed would permit release of intimate details concerning persons who could be readily identified by those familiar with the situation, notwithstanding the deletions, thus exposing the individuals to embarrassment or possible reprisals.[7] The District Judge, without explanation, denied the government motion for clarification.[8] Pending appeal he granted a stay.

II. EXEMPTION 6: PERSONNEL, MEDICAL, AND SIMILAR FILES

The FOIA was enacted to ensure public access to a wide range of government reports and information.[9] Recognizing that in certain circumstances disclosure realistically would not be in the public interest, Congress attempted to delineate a series of narrow exemptions.[10] The sixth exemption provides that disclosure is unnecessary if the matters are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." [11]

The District Court held that exemption 6 "has no application to this investigatory report." This holding was based on the view that the exemption "was designed to apply to detailed personal resumes and health records from agencies such as the Veterans Administration, welfare departments and the military." [12] We think this statutory interpretation incorrect. We hold that exemption 6 is applicable to material such as the report here, hence we reverse the District Court and remand for appropriate review.

[1, 2] While the District Judge provided no elaboration of his rationale in the form of findings, he implied that the report here could not be considered "similar files" under exemption 6. Looking to the purpose of exemption 6, on the contrary, we believe that the investigatory report comes well within the ambit of exemption 6. That exemption was designed to protect individuals from public disclosure of intimate details of their lives, whether the disclosure be of personnel files, medical files, or other similar files.[13] The exemption is not limited to Veterans' Administration or Social Security files, but rather is phased broadly to protect individuals from a wide range of embarrassing disclosures.[14] As the materials here contain information regarding marital status, legitimacy of children, identity of fathers of children, medical condition, welfare payments, alcoholic consumption, family fights, reputation, and so on, it appears that the report involves sufficiently intimate details to be a "similar" file under exemption.[15]

Of course, our interpretation of the statute, concluding that the investigatory report comes within the class of similar files which exemption 6 aimed at protecting, does not resolve the question whether exemption 6 dictates nondisclosure

---

[7] Affidavit of Inspector General Kossack of 15 May 1973, in Appendix at 72–74.

[8] District Court Order of 5 June 1973, in Appendix at 76.

[9] 5 U.S.C. § 552(a). *See generally* EPA v. Mink, 410 U.S. 73, 79–80, 93 S. Ct. 827, 35 L. Ed. 2d 119 (1973).

[10] 5 U.S.C. § 552(b).

[11] 5 U.S.C. § 552(b)(6).

[12] Appendix at 67.

[13] The House Report on S. 1160, the bill which became the Freedom of Information Act, explains the broad purpose of exemption 6:

> Such agencies as the Veterans' Administration, Department of Health, Education, and Welfare, Selective Service, and Bureau of Prisons have great quantities of files containing intimate details about millions of citizens. Confidentiality of these records has been maintained by agency regulation but without statutory authority. A general exemption for the category of information is much more practical than separate statutes protecting each type of personal record. The limitation of a "clearly unwarranted invasion of personal privacy" provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to Government information by excluding those kinds of files the disclosure of which might harm the individual. The exemption is also intended to cover detailed Government records on an individual which can be identified as applying to that individual and not the facts concerning the award of a pension or benefit or the compilation of unidentified statistical information from personal records.—H.R. Rep. No. 1497, 89th Cong., 2d Sess. 11 (1966) (citation omitted).

[14] Furthermore, the exemption should be read in conjunction with 5 U.S.C. § 552(a)(2), which provides that

> To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction. However, in each case the justification for the deletion shall be explained fully in writing.

[15] This was not controverted in RHA's brief, which assumed arguendo that the files were "similar files." Brief for Appellee at 16.

here, for exemption 6 specifically permits protection only of those files whose disclosure would result in "a clearly unwarranted invasion of personal privacy." [16] On remand, it is for the District Judge to determine whether the files fall within that category.

[3] In an opinion by Judge Wright, this court has previously considered the scope of the "clearly unwarranted invasion" language, in Getman v. NLRB.[17] We held that exemption 6 involves a balancing of the interests of the individuals in their privacy against the interests of the public in being informed. We noted that the statute "instructs the court to tilt the balance in favor of disclosure." [18]

Specifically we suggested that in balancing interests the court should first determine if disclosure would constitute an invasion of privacy, and how severe an invasion. Second, the court should weigh the public interest purpose of those seeking disclosure, and whether other sources of information might suffice. Such balancing is unique for exemption 6; normally no inquiry into the use of information is made, and the information is made available to any person.[19]

[4] These principles should be applied in evaluating the investigatory reports at issue here.[20] The District Court should first determine the nature and extent of the invasion of the individuals' privacy.[21] It should then consider the public interest purpose of RHA, and whether it could be achieved without this material. A balancing of these factors must thereafter be made.

One important factor which must be considered on remand is whether the deletions thus far ordered are sufficient to protect the privacy of the individuals. In construing the various exemptions, this court has often suggested deletions of certain protected matters so that the remainder of the document could be disclosed.[22] The affidavit of Inspector General Kossack states, however, that the court order does not order adequate deletions, and that enough highly confidential material is left which would enable people with knowledge of the area to determine the identity of the individuals involved.[23] The District Judge did not respond to this affidavit nor make any change in his order. On remand, the District Judge should reconsider and reevaluate this affidavit, and Kossack's prior affidavit submitted before the court's decision.[24]

The District Judge should also consider any alternative sources of information which might be available. For example, the possibility of RHA asking individuals independently for similar information should be explored.[25]

III. EXEMPTION 4: CONFIDENTIAL OR PRIVILEGED FINANCIAL INFORMATION

The USDA argues that exemption 4 also protects the investigatory report from disclosure. This exemption applies to "trade secrets and commercial or financial information obtained from a person and privileged or confidential." [26] The trial court held that the exemption "was designed to protect the privacy and competitive position of the individual [27] . . . and since the contents of this report do not fit the description in this exemption, it is inapplicable to the instant report. Since all names and other identifying features can be deleted, any remaining financial information will be in the nature of a statistical report." [28]

[5, 6] While it is true that exemption 4 is primarily a trade secrets exemption, it also protects individuals from disclosure of financial information which is

---

[16] 5 U.S.C. § 552(b)(6).
[17] 146 U.S. App. D.C. 209, 450 F. 2d 670 (1971).
[18] 146 U.S. App. D.C. at 213, 450 F. 2d at 674.
[19] 146 U.S. App. D.C. at 213 n. 10, 450 F. 2d at 674 n. 10.
[20] Although *Getman* simply involved disclosure of names and addresses of employees, its principles have wide-ranging applicability.
[21] The District Court might include a consideration of whether the individuals expected confidential treatment.
[22] See, for example, two cases dealing with exemption 4, Grumman v. Renegotiation Board, 138 U.S. App. D.C. 147, 149–150, 425 F. 2d 578, 580–581 (1970); Bristol-Myers v. FTC, 138 U.S. App. D.C. 22, 26, 424 F. 2d 935, 939 (1970).
[23] Affidavit of Inspector General Kossack of 15 May 1973, in Appendix at 73.
[24] As indicated *supra*, Mr. Kossack submitted one affidavit to the District Court on 29 January 1973, and one on 15 May 1973. The District Court's judgment was handed down on 9 May 1973.
[25] We deal with the Government's suggestion that authorizations for release be obtained by RHA from individuals involved in Part V *infra*. That is different from the suggestion we make here of discussions with individuals independent from the USDA investigation and report.
[26] 5 U.S.C. § 552(b)(4).
[27] The District Court here cited Bristol-Myers v. FTC, 424 F. 2d at 938, which stated that the aim of the exemption was "protecting the privacy and the competitive position of the citizen who offers information to assist government policy makers."
[28] Appendix at 67.

privileged or confidential. This court has recently described the scope and meaning of "confidential" in exemption 4 in National Parks & Conservation Association v. Morton. Judge Tamm concluded that,

> commercial or financial matter is "confidential" for purposes of the exemption if disclosure of the information is likely to have either of the following effects: (1) to impair the Government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained.[29]

As much of the information collected here related to loan applications, certainly some data is financial information which might merit confidential treatment.[30] Of course a bare claim by an interested government agency of confidentiality is not sufficient.[31] However, the listing of information obtained strongly suggests the accuracy of USDA's conclusion that the information is "implicitly and unquestionably not the kind of information which would customarily be released to the public by the persons from whom it was obtained." [32] Contrary to the trial court, we regard exemption 4 as applicable.

[7] We therefore remand to the District Court for reconsideration of exemption 4 for reasons similar to those discussed regarding exemption 6. While several of our Circuit's cases support the idea of deletions to permit disclosure of the remainder of the report,[33] we fear that the deletions made by the District Judge do not adequately deal with the rather detailed reasons of the Inspector General that the deletions are ineffective to protect the privacy and confidentiality of the individuals involved.[34]

IV. EXEMPTION 7: INVESTIGATORY FILES

This provision exempts from disclosure "investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency." [35] The District Court held that USDA "failed to make the requisite showing of imminent adjudicatory proceedings or the concrete prospect of enforcement proceedings," [36] and hence the files were not protected by exemption 7.

Since this decision on May 9, 1973 this Circuit has extensively considered exemption 7 in two cases, Weisberg v. U.S. Department of Justice,[37] and Aspin v. Department of Defense.[38] We remand to the District Court for reevaluation of the applicability of exemption 7 in the light of these opinions and our comments hereafter.

The standard used by the District Judge is no longer proper under the *Weisberg* and *Aspin* decisions. In *Weisberg*, where FBI materials concerning the investigation of President Kennedy's death were sought, we held in an *en banc* decision by Judge Danaher that the files were exempt from disclosure because they were investigatory files compiled for law enforcement purposes.[39] Despite the fact that no prosecution or other such method of law enforcement was undertaken or pending, the files remained exempt from disclosure. The focus was on "how and under what circumstances the files were compiled . . . ." [40]

In *Aspin*, decided one month after *Weisberg*, Judge Tamm's opinion for the court provided a more detailed analysis of exemption 7. The material at issue in *Aspin* was the report of the Peers Commission, which investigated the My Lai incident and subsequent Army investigation, with emphasis on evidence of possible offenses under the Uniform Code of Military Justice and possible future prosecution. Judge Tamm noted that the duty of the trial court was to "examine the total record to determine 'whether the files sought . . . relate

---

[29] No. 73-1033 (1974), 162 U.S. App. D.C. ——, ——, 498 F. 2d 765, 770 (citation omitted).

[30] The Senate Report on the bill which became FOIA suggests that loan applications would be within the scope of exemption 4. S. Rep. No. 813, 89th Cong., 1st Sess. 9 (1965).

[31] Bristol-Myers v. FTC, 138 U.S. App. D.C. at 25, 424 F. 2d at 938.

[32] Affidavit of Inspector General Kossack of 29 January 1973, in Appendix at 44.

[33] *See* note 22 *supra*. *See also* National Parks & Conservation Association v. Morton, No. 73-1033, 162 U.S. App. D.C. ——, ——, 498 F. 2d 765, 770 (1974).

[34] *See* n. 77 *supra*.

[35] 5 U.S.C. § 552(b)(7).

[36] District Court Order in Appendix at 67, *citing Bristol-Myers*.

[37] 160 U.S. App. D.C. 71, 489 F.2d 1195 (1973) (en banc), cert. denied, 42 U.S.L.W. 3627, 416 U.S. 993, 94 S. Ct. 2405, 40 L. Ed. 2d 772 (1974).

[38] 160 U.S. App. D.C. 231, 491 F. 2d 24 (1973). Still more recently we have considered exemption 7 in Center for National Policy Review v. Weinberger, No. 73-1090, 163 U.S. App. D.C. ——, 502 F. 2d 370 (1974).

[39] The court relied heavily on the Attorney General's determination, and the District Court review of that determination. No *in camera* inspection was undertaken by either court.

[40] 160 U.S. App. D.C. at 78, 489 F. 2d at 1202.

to anything that can fairly be characterized as an enforcement proceeding.' " [41] The Peers Commission Report, conducted with a view of court-martial proceedings, did meet this test and hence came within the exemption.

In *Aspin* the purposes of exemption 7 were identified: the prevention of premature disclosure of an investigation's results, and the maintenance of confidentiality of both the procedures of investigation and the witnesses' revelations.[42] These purposes compelled us there to conclude that the termination of enforcement proceedings was not a cause for withdrawal of exemption 7 protection.[43] Additionally, our decision in *Weisberg* has made clear that exemption 7 protection does not end "when there is no longer any prospect for future enforcement proceedings (necessitated in *Weisberg* by the death of the only suspect) . . . ." [44]

[8] It is established now that the Government need not show "imminent adjudicatory proceedings or the concrete prospect of enforcement proceedings." What the Government *is* required to show is that the investigatory files were compiled *for adjudicative or enforcement purposes*. Whether the adjudication or enforcement has been completed is not determinative, nor is the degree of likelihood that the adjudication or enforcement may be imminent, as the District Judge here thought before *Weisberg* and *Aspin*. Here the investigation was undertaken to determine whether USDA's FmHA had engaged in racial discrimination. As a result of the investigation, USDA concluded that there had been no discrimination, and naturally there have been no enforcement proceedings. This result does not alter the basic inquiry when exemption 7 is claimed: was it an investigation "for law enforcement purposes"? To put the question another way, with specific applicability to the case here: is an agency's internal monitoring to insure that its employees are acting in accordance with statutory mandate and the agency's own regulations and investigation "for law enforcement purposes" within the meaning of exemption 7?

On its face, exemption 7's language appears broad enough to include all such internal audits. If this broad interpretation is accepted, however, we immediately encounter the problem that most information sought by the Government about its own operations is for the purpose ultimately of determining whether such operations comport with applicable law, and thus is "for law enforcement purposes." Any internal auditing or monitoring conceivably could result in disciplinary action, in dismissal, or indeed in criminal charges against the employees. But if this broad interpretation is correct, then the exemption swallows up the Act; exemption 7 defeats one central purpose of the Act to provide public access to information concerning the Government's own activities.

We think "investigatory files compiled for law enforcement purposes" must be given the same meaning, or a meaning to achieve the same result, whether the subject of the files is a government employee or an ordinary private citizen. While Congress did not confront this problem specifically, the examples cited of "investigatory files" and "law enforcement purposes" point to this interpretation.[45] For the purpose of analyzing the application of exemption 7 in the

---

[41] 160 U.S. App. D.C. at 234, 491 F. 2d at 27 (citation omitted).

[42] 491 F. 2d at 29, *citing* Frankel v. SEC, 460 F. 2d 813 (2d Cir.), cert. denied, 409 U.S. 889, 93 S. Ct. 125, 34 L. Ed. 2d 146 (1972). We referred to Chief Judge Bazelon's suggestion in *Bristol-Myers* that the District Court should determine whether the prospect of enforcement proceedings is concrete enough to bring into operation the exemption. . . ." 424 F. 2d at 939–940. (This phraseology was adopted by the District Court in the case at bar.) We distinguished the My Lai investigation, where courts-martial had been held, from the *Bristol-Myers* situation, where the Federal Trade Commission had made a conscious decision *not* to maintain any enforcement proceeding at least two years prior to suit to compel disclosure of the documents. The question in that case was, therefore, whether the bare assertion by an agency that files were compiled for law enforcement purposes *when no enforcement proceedings were in fact ever prosecuted*, would be enough to preclude disclosure. The court held that such an assertion was not sufficient, and remanded for further consideration in the trial court.—491 F. 2d at 29 (citations omitted; emphasis original). We thus concluded in *Aspin* that the District Court's reliance on *Bristol-Myers* was misplaced.

[43] "[I]f investigatory files were made public subsequent to the termination of enforcement proceedings, the ability of any investigatory body to conduct future investigations would be seriously impaired. Few persons would respond candidly to investigators if they feared that their remarks would become public record after the proceedings. Further, the investigative techniques of the investigating body would be disclosed to the general public." 491 F. 2d at 30.

[44] *Aspin*, 491 F. 2d at 30.

[45] The Senate Report states that "investigatory files compiled for law enforcement purposes" are "files prepared by Government agencies to prosecute law violators." S. Rep. No. 813, 89th Cong., 1st Sess. 9 (1965). No distinction is drawn between violators who are government employees and violators who are private citizens. *See also* H. R. Rep. No. 1497, 89th Cong., 2d Sess. 11 (1966).

instant and similar cases, it is therefore necessary to distinguish two types of files relating to government employees: (1) government surveillance or oversight of the performance of duties of its employees; (2) investigations which focus directly on specifically alleged illegal acts, illegal acts of particular identified officials, acts which could, if proved, result in civil or criminal sanctions.[46] The applicability of exemption 7 to each individual case is to be ascertained by making a careful distinction between these two categories.[47]

[9–11] The purpose of the "investigatory files" is thus the critical factor. Was the purpose of the disputed report here to determine if grounds existed for bringing a civil rights action against the loan officer? If the purpose of the investigation was to consider an action equivalent to those which the Government brings against private parties, thus demonstrating that the "law enforcement purpose" was not customary surveillance of the performance of duties by government employees, but an inquiry as to an identifiable possible violation of law, then such inquiry would have been "for law enforcement purposes" whether the individual were a private citizen or a government employee. But was this the purpose of the investigation here? On this record we cannot say, and hence our consideration of the applicability of exemption 7 likewise calls for a remand to the trial court for inquiry as to this[48] and other relevant points.

V. EFFECT OF INDIVIDUAL'S CONSENT TO GOVERNMENT DISCLOSURE

The Government has offered to release information concerning any individual to RHA if the written authorization of the individual is obtained. Specifically, the Government wrote to RHA: If you furnish us with appropriate written authorizations from those individuals who, to your present knowledge, furnished information in this investigation, we will consider making available information furnished by any such individual.[49]

RHA did not obtain any individual releases.

The exemptions to the Freedom of Information Act place limits on compulsory disclosure; presumably the Government has power to waive an exemption. However, in so doing, the Government and a court, when its authority is invoked, must be alert to protect other interests in confidentiality besides those of the Government which are present in each of the nine exceptions, some more obviously than others. Much information is disclosed voluntarily and involuntarily (but with less difficulty than would otherwise be true), because the individuals supply the information believe that, since the Government has power to protect confidentiality under the exemptions, it will do so.

This suggestion of the Government for obtaining individual releases protects the interests involved in exemption 6 that individual's medical, personnel, or similar files not be indiscriminately disclosed. However, the ambiguous terms of the Government's offer to release should be clarified. It is unclear whether the Government would release personal information about one person which is

---

[46] The character of the statute violated would rarely make a material distinction, because the law enforcement purposes protected by exemption 7 include both civil and criminal purposes, *e.g.*, civil rights, as here. *See* H.R. Rep. No. 1497, 89th Cong., 2d Sess. 11 (1966): This exemption covers investigatory files related to enforcement of all kinds of laws, labor and securities laws as well as criminal laws. This would include files prepared in connection with related Government litigation and adjudicative proceedings. S. 1160 is not intended to give a private party indirectly any earlier or greater access to investigatory files than he would have directly in such litigation or proceedings.—*Cf.* Evans v. Department of Transportation, 446 F. 2d 821 (5th Cir.), cert. denied, 405 U.S. 918, 92 S. Ct. 944, 30 L. Ed. 2d 788 (1972).

[47] The distinction was also drawn in Center for National Policy Review v. Weinberger, No. 73–1090, 163 U.S. App. D.C. ——, 502 F. 2d 370 (1974), where Judge Leventhal wrote for the court. There is no clear distinction between investigative reports and material that, despite occasionally alerting the administrator to violations of the law, is acquired essentially as a matter of routine. What is clear, however, is that where the inquiry departs from the routine and focuses with special intensity upon a particular party, an investigation is under way.—*Id.* at ——, 502 F. 2d at 373. Judge Leventhal separately analyzed the meaning of the phrases "investigatory files" and "law enforcement purposes." We have not found such separation necessary here, but have dealt with the elements as they "fuse and interact." *Id.* at ——, 502 F. 2d at 374.

[48] In so determining, a court must of course be wary of self-serving declarations of any agency; it must be clear to the court that more than ephemeral possibilities of enforcement were anticipated by the agency in undertaking the investigation. If an investigatory file is compiled for the purpose of determining whether a law enforcement proceeding should be brought (in the same manner as against a private citizen) and against whom, then, whether the agency concludes that proceedings are necessary or not, the agency may utilize exemption 7 to protect its investigatory process and sources.

[49] Appendix at 44.

furnished by a second person on simply the second's authorization, or only by the first's, or by both. One interest protected by exemption 7, that of enabling the investigatory process to proceed unimpeded by hesitancy of witnesses or disclosure of investigatory technique, which was not previously evaluated by the trial court, should not be overlooked on remand.

The trial court should weigh carefully several difficulties inherent in the release by individual consent of government compiled information on private individuals. First, if many consent, there may be explicit or implicit group pressure on those few who do not wish to have their lives publicized. Second, there may be pressure by the RHA or other groups to force individuals to comply. We impute no bad motives or actions to RHA; we merely state a possibility true for any interested organization. Third, if many consented-to disclosures are made, it may become significantly easier to identify the remainder of the group because of the smaller size of unknowns.

Finally, putting the same amount of information in the public domain could be achieved by private interviewing of those individuals who wish to participate. They can then reveal whatever information they desire, and this process might, as a practical matter, be no more time-consuming for RHA than obtaining formal consents to disclosure by the government. This approach would be similar to the approach taken for grand jury witnesses. We do not allow a grand jury witness' testimony to be revealed except under well-defined rules; however, the witness is usually free to come out of the grand jury and tell the public what he knows with regard to the subject of the grand jury inquiry.

VI. CONCLUSION

We remand this case to the District Court for reconsideration of exemptions 4, 6, and 7, in light of this opinion. In so doing, we need not now confront the question of equitable discretion of the court to go beyond FOIA, which was suggested by USDA. We also do not consider the applicability of exemption 5,[50] as the Government has not objected to the District Court's holding that this exemption is inapplicable.

Reversed and remanded.

RURAL HOUSING ALLIANCE

v.

UNITED STATES DEPARTMENT OF AGRICULTURE ET AL., APPELLANTS

No. 73-1771

UNITED STATES COURT OF APPEALS, DISTRICT OF COLUMBIA CIRCUIT,
SEPTEMBER 24, 1974

Before BAZELON, Chief Judge, and ROBB and WILKEY, Circuit Judges.

ORDER

Per Curiam.

On consideration of appellee's petition for rehearing, it is

Ordered by the Court that the aforesaid petition for rehearing is denied.

BAZELON, Chief Judge, concurring in the denial of appellee's motion for rehearing:

As initially issued, the court's opinion in this case contained the following paragraph:

"We refer RHA's suggestions of counsel's participation in in camera inspection to the District Judge on remand. Such participation by counsel may be allowed by the District Judge in his discretion, if he finds such participation necessary to his comprehension of the arguments and thus to a fair and correct resolution of this case."

On the Government's motion, the court ordered deletion of this paragraph over my dissent. Two reasons have been given for the deletion: (1) that the paragraph was incorrect as a matter of law; (2) that it was unnecessary. I join in the denial of appellee's present motion for rehearing solely on the second ground.

---

[50] We have recently had occasion to consider exemption 5 in Montrose Chemical Corporation v. Train, 160 U.S. App. D.C. 270, 491 F. 2d 63 (1974).

The court today agrees that the deleted passage was unnecessary to its decision. Accordingly, the court's action does not decide the question which the passage addressed.

ROBB, Circuit Judge:

I voted to delete the paragraph referred to by Judge Bazelon on two grounds: (1) the paragraph was an incorrect statement of the law, and (2) it was unnecessary to the decision.

ERNESTINE ROBLES ET AL., APPELLANTS,

v.

ENVIRONMENTAL PROTECTION AGENCY, APPELLEE.

No. 72-2470

UNITED STATES COURT OF APPEALS, FOURTH CIRCUIT

ARGUED APRIL 3, 1973—DECIDED SEPT. 11, 1973

Action seeking disclosure of information. The United States District Court for the District of Maryland, Herbert F. Murray, J., held the information to be exempt and plaintiffs appealed. The Court of Appeals, Donald Russell, Circuit Judge, held that information gathered by Environmental Protection Agency and relating to homes where uranium tailings had been used for fill was not exempt from disclosure.

Reversed and remanded.

Widener, Circuit Judge, filed concurring and dissenting opinion.

1. Records ⇐ 14

Freedom of Information Act exemption relating to personnel and medical and similar files indicates that, while exemption is not limited to strictly medical or personnel files, to be exempt similar files must have same characteristics of confidentiality that ordinarily attach to information in medical or personnel files. 5 U.S.C.A. § 552(b)(6).

2. Records ⇐ 14

In determining whether Freedom of Information Act exemption relating to files which are similar to personnel and medical files applies to particular information courts tilt balance in favor of disclosure. 5 U.S.C.A. § 552(b)(6).

3. Records ⇐ 14

Promise of confidentiality made at time information was gathered may be factor in determining whether information is exempt from disclosure as information similar to that contained in personnel and medical files but such promise is not enough to defeat right of disclosure. 5 U.S.C.A. § 552(b)(6).

4. Records ⇐ 14

Promise of confidentiality made in connection with gathering information relating to buildings would be entirely inapplicable to claim of right to disclosure of information relating to public buildings. 5 U.S.C.A. § 552(b)(6).

5. Records ⇐ 14

Interest of parties seeking disclosure of information has no bearing on right to disclosure. 5 U.S.C.A. § 552.

6. Records ⇐ 14

Claim that disclosure of information would do more harm than good did not warrant withholding information which was gathered by Environmental Protection Agency relating to homes which had used tailings from uranium processing as fill. 5 U.S.C.A. § 552.

7. Records ⇐ 14

Fact that information sought was of such scientific nature that ordinary citizen could not properly evaluate or understand it did not preclude disclosure under Freedom of Information Act. 5 U.S.C.A. § 552.

8. Records ⇨ 14

Right to disclosure under Freedom of Information Act is not to be resolved by balance of equities or weighing of need or even benefit. 5 U.S.C.A. § 552.

9. Records ⇨ 14

Information which was gathered by Environmental Protection Agency and which related to homes where uranium tailings had been used for fill was not exempt from disclosure under Freedom of Information Act. 5 U.S.C.A. § 552.

Victor H. Kramer, Washington, D.C. (Richard B. Wolf, Washington, D.C., and Joel Zeldin, on brief) for appellants.

Andrew J. Graham, Asst. U.S. Atty. (George Beall, U.S. Atty., on brief), for appellee.

Before Craven, Russell and Widener, Circuit Judges.

Donald Russell, Circuit Judge:

This is a bizarre case, illustrative of the ignorance by even scientists of the dangerous properties of radioactive waste materials and of the hazards that may result from such ignorance. It arose out of the practice by a uranium processing plant of making available free of charge its uranium tailings[1] for use as clean fill dirt in connection with construction of private and public structures in the community of Grand Junction, Colorado, where the uranium processing plant was located. The practice, begun in 1950, continued until 1966, when the hazards incident to the use of such tailings were belatedly recognized. In the meantime, these tailings had been extensively used. Because of the obvious dangers connected with such use, the Environmental Protection Agency (hereinafter referred to as EPA), with the assistance of the Colorado Department of Health, undertook in 1970 to monitor the radiation levels in the homes and public structures where any of these tailings had been used. In addition, the homes and business or public structures were tested for radioactive emissions. In the course of this monitoring, some 15,000 homes were surveyed. The survey was extensive. In some of the homes an air sampler was placed for a week at a time on each of six occasions in the course of a year as a part of what was described as an "(I)ndoor radon daughter concentration level." In order to secure approval for such a survey from a homeowner, the government surveyors were instructed to advise orally the homeowner or occupier that the results of the survey would not be released to any one other than the owner or occupier and federal officials working on the problem. When the surveys were completed, the results were made available by the EPA to the Colorado Department of Health, in conjunction with which the survey was made. Through an arrangement with the Colorado Department of Health, the Development Director of the community can secure and make available to any "proper party" the results of the tests made on any specific structure. In addition, each owner of a structure surveyed has been given the results of the survey of his building.

The plaintiffs at first made formal request upon the defendant for the results of the survey as it applied to all public and private structures in the community. It later modified this request to cover only those structures in which the radiation levels exceeded the Surgeon General's "safety guidelines". The agency responded to this request by offering to provide the results but with the names and addresses of homeowners or occupiers deleted. It based its refusal to supply any of this information upon the exemptions set forth in subdivisions (4) and (6) of Section 552(b), 5 U.S.C. This was unacceptable to the plaintiffs, who then filed this action under the Freedom of Information Act[2] to compel disclosure. The defendant entered a motion to dismiss, and, in the alternative, a motion for summary judgment. The plaintiffs then submitted their cross-motion for summary judgment. When the motions came on for hearing, the District Court denied plaintiffs' cross-motion and granted the defendant's motion for summary judgment, finding that disclosure, though not exempt under subdivision (4), was exempted under subdivision (6) of the Act. The plaintiffs appeal.

On this appeal, the defendant agency apparently concedes that it is obligated to disclose to the plaintiffs, without regard to their interest or want of interest, the information requested unless disclosure is "specifically" excused under one of the nine express exemptions set forth in the Freedom of Information Act,

---

[1] These tailings are described as a sand-like by-product of the uranium processing plant's mining operations.

[2] 5 U.S.C., Section 552, *supra*.

and that, in asserting an excuse for disclosure under any express exemption, "the burden is on" it "to sustain its action." Whether conceded or not, this is the clear purport of the Act itself. Epstein v. Resor (9th Cir. 1970) 421 F.2d 930, 933, cert. denied 398 U.S. 965, 90 S.Ct. 2176, 26 L.Ed.2d 549. While it sought to excuse nondisclosure in this case under both exemptions (4) and (6) of the Act, its claim under (4) was disallowed by the District Court and, in this Court, the agency rests its right wholly upon exemption (6). Accordingly, the sole issue here is whether the District Court was correct in finding that the defendant agency had sustained its burden of establishing a right to exemption from disclosure of the requested information under exemption (6) of the Act.

Exemption (6) is as follows:

"(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;".

[1] Obviously, the information requested was not included in any "personnel" or "medical" files as such. The basis for a claim of exemption must accordingly be found in the phrase, "similar files the diclosure of which would constitute a clearly unwarranted invasion of personal privacy." The term "similar" was used, it seems, to indicate that, while the exemption was not limited to strictly medical or personnel files, the files covered in this third category must have the same characteristics of confidentiality that ordinarily attach to information in medical or personnel files; that is, to such extent as they contain " 'intimate details' of a 'highly personal' nature", they are within the umbrella of the exemption. This is the real thrust of the exemption as it was construed in Getman v. N.L.R.B. (1971), 146 U.S.App.D.C. 209, 450 F.2d 670, 675. See, Note, Invasion of Privacy and the Freedom of Information Act: Getman v. N.L.R.B., 40 Geo.Wash.L.Rev. 527, 532 (1972). It would seem to follow that the exemption applies only to information which relates to a specific person or individual, to "intimate details" of a "highly personal nature" in that individual's employment record or health history or the like, and has no relevancy to information that deals with physical things, such as structures as in this case.[3] The agency contends, however, that this is too simplistic an approach to the unique situation in this case. It is true, the agency argues, that, while the information sought by the plaintiffs relates strictly to the condition of structures, of buildings, and real estate, it was gathered, analyzed, and is of interest only as it relates to the possible effect of that condition on the health and well-being of the occupants of those structures, *i.e.*, of specific persons and individuals. So viewed, in this broad context, the information, the agency contends, comes within the definition of information of a "highly personal nature", as contemplated in exemption (6).

It must be conceded that there is a certain persuasiveness to this argument. The survey of the homes in the community was engaged in because of concern for personal health and safety; it was not an engineering survey to determine the structural adequacy or nature of the structures. And the reason for the health concern was the possibility that continued occupancy of the building might expose the occupants and even their progeny to hazards of health and even biological impairments. It is suggested that these potential health impairments could affect adversely employment opportunities and might even reduce marriage possibilities of the occupants.

[2] Assuming, however, that it is possible to analogize these records to health records, it does not follow automatically that such records are exempt from disclosure. The statutory exemption does not simply cover any files that may be regarded as "similar" to health files. "Similar files", in order to qualify under the exemption, must fit the additional qualifications set forth in the exemption, *i.e.*, they must contain information "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." [4] The use of the term "clearly" in this qualification, which was not inadvertent but purposeful on the part of Congress, was, itself, a "clear" instruction to the Courts that, in determining the issue whether a disclosure would constitute "a clearly unwarranted invasion of personal privacy", they should "tilt the balance in favor of disclosure". Getman v. N.L.R.B. *supra*, at 674 of 450 F.2d.

---

[3] *Cf.*, the language of Professor Davis in Administrative Law, 1970 Supp., Section 3A.22 at 164, where, in discussing exemption (6) and particularly the qualifying term "personal privacy", he says: "I think 'personal privacy' always relates to individuals."

[4] One commentator has found this language unsatisfactory, adding that: "The ambiguous wording of exemption 6 and the traditional problems in securing the right to privacy may preclude creation of a completely satisfactory test." 40 Geo. Wash. L. Rev. 527, at p. 540 (1972).

[3, 4] In resolving against disclosure, the District Court relied strongly on the fact that the agency had in some instances promised the householder that the results of the survey would be kept confidential. While, perhaps, promise of confidentiality is a factor to be considered, it is not enough to defeat the right of disclosure that the agency "received the file under a pledge of confidentiality to the one who supplied it. Undertakings of that nature cannot, in and of themselves, override the Act." Ackerly v. Ley (1969), 137 U.S.App.D.C. 133, 420 F.2d 1336, 1339–1340, n. 3; Legal Aid Society of Alameda County v. Shultz (D.C.Cal.1972) 349 F.Supp. 771, 776; *Davis, supra*, at 164. Particularly in this case is the alleged promise of confidentiality unavailing as an excuse. In the first place, the promise was given by the door-to-door surveyors only where confidentiality was specifically inquired about by a householder. The agency has offered no proof of how many householders in the community had received such promise. Even more important is the fact that the information has not been held in confidence. The results of the survey are available to the Colorado Department of Health. This Department, seemingly with the approval of EPA, readily makes available on request the results of the survey as to any specific structure through the City Director of Development.[5] This practice is well known to the EPA, which offers proof of the practice in support of its claim to exemption by reason of its promise of confidentiality. And it is of some significance that, so far as the record indicates, no householder has objected to this disclosure by the City Director of Development. Finally, it should be pointed out that this claim, that a promise of confidentiality supports the award of an exemption, is entirely inapplicable to public buildings.

[5] Another reason urged by the agency for its denial of disclosure is that the need of the public, as well as the interest of the plaintiffs, in securing the information "is negligible." This argument misconceives the plain intent of the Act. As Professor Davis has so convincingly emphasized, the earlier provision in the Administrative Procedure Act "provided for disclosure 'to persons properly and directly concerned.' That was changed to 'any person' ", demonstrating beyond argument that disclosure was never to "depend upon the interest or lack of interest of the party seeking disclosure." *Davis, supra*, Section 3A.4 at 120;[6] Bannercraft Clothing Company v. Renegotiation Board (1972) 151 U.S.App.D.C. 174, 466 F.2d 345, 352, n. 6, cert. granted 410 U.S. 907, 93 S.Ct. 967, 35 L.Ed.2d 269; Sterling Drug, Inc. v. F.T.C. (1971), 146 U.S.App.D.C. 237, 450 F.2d 698, 705; Skolnick v. Parsons (7th Cir. 1968) 397 F.2d 523, 525.

[6] Equally unpersuasive is the argument that disclosure should be refused because it "would do more harm than good". Such an argument has nothing to do with "personal privacy" but is rather an argument that courts, in disposing of actions under the Act, may exercise discretion to grant or deny equity relief. While such argument has received some limited support, the better reasoned authorities find no basis for this balancing of equities in the application of the Act; indeed, the very language of the Act seems to preclude its exercise. Wellford v. Hardin (4th Cir. 1971) 444 F.2d 21, 24–25; Soucie v. David (1971) 145 U.S.App. D.C. 144, 448 F.2d 1067, 1077; Getman v. N.L.R.B., *supra*, at 677 of 450 F.2d; and Bannercraft Clothing Co. v. Renegotiation Board, *supra*, at 353 of 466 F.2d; *cf.*, however, General Services Administration v. Benson (9th Cir. 1969) 415 F.2d 878, 880, and Davis, *supra*, Sec. 3A.6, pp. 123–4.[7] Moreover, the claim of public harm is at best ambiguous. The only harm suggested by the agency involves the individuals whose homes were surveyed. Presumably, these individuals knew of

---

[5] *Cf.*, Wellford v. Hardin (D.C. Md. 1970) 315 F. Supp. 175, 178, aff'd (4th Cir.) 444 F. 2d 21.

[6] In further elaboration on this point, Professor Davis, in his authoritative text, has said, at 121:

"* * * For instance, the sixth exemption in subsection (e) authorizes withholding of medical files if disclosure 'would constitute a clearly unwarranted invasion of personal privacy.' If the officer or judge finds that the disclosure will be an unwarranted invasion but is in doubt whether it is 'clearly unwarranted,' a natural approach to decision would be to weigh the privacy interest against the interest of the party seeking the information, so that disclosure would be made to one with a legitimate need but not to one who is malevolently motivated or an officious intermeddler. But under the Act such a balancing is inappropriate. All parties are equal in satisfying the words 'any person.' "

[7] *Benson* states the role of the court in actions under the Act as follows:

"In exercising the equity jurisdiction conferred by the Freedom of Information Act, the court must weigh the effects of the disclosure and nondisclosure, according to the traditional equity principles, and determine the best course to follow in the given circumstances. The effect on the public is the primary consideration." (415 F. 2d at 880).

the practice of the City Development Director of making available the information in question to any proper person requesting it. Yet no concerned individual, so far as this record shows, has ever objected; nor has the defendant agency instanced one case in which an individual householder has complained of any harm suffered by him as a result of disclosure. Nor, for that matter, has the defendant agency attempted in this case to show that any "specific governmental interests" will be harmed by the disclosure requested by the plaintiffs. *Cf.* Bristol-Meyers Company v. F.T.C. (1970) 138 U.S.App.D.C. 22, 424 F.2d 935, 938, cert. denied 400 U.S. 824, 91 S.Ct. 46, 27 L.Ed.2d 52.

[7] The agency suggests that the information sought is of such a recondite scientific nature that the ordinary citizen could not properly evaluate or understand it. No one would question the ignorance of the general public—and perhaps, the scientific world, too—as to the possible harmful aspects of radioactive materials. The same could no doubt be said of much governmental information. Even census data is subject to misinterpretation and has prompted violent controversy even among experts. But the mere circumstance that information may not be fully understood is not among the "specific" exemptions authorized under the Act. Actually, it may well be that the very fact that the government so adamantly opposes release may give free rein to unbridled fear for the worst on the part of the people of this community; whereas, the release of the surveys, even though not fully understood, may have a beneficial, calming effect on the reasonable apprehensions of these citizens.

[8] The Government has, it developed, embarked recently since discovery of the danger on a remedial program intended to remove or minimize the hazard of radioactive injury to the occupiers of these structures. The District Court felt that such a program militated against a determination that there was any public need for or benefit to result from disclosure. In balancing equities, it thought this of moment. But, as we have already observed, the right to disclosure under the Act is not to be resolved by a balancing of equities or a weighing of need or even benefit. The only ground for denial of disclosure in this situation is that the disclosure would represent a "clearly unwarranted invasion of personal privacy." For the reasons given we are unable to find any reasonable basis for finding such a "clearly unwarranted basis."

[9] Reversed, with direction to the District Court to enter a decree granting disclosure as provided in Section 552, 5 U.S.C.

WIDENER, Circuit Judge (concurring and dissenting):

I must respectfully dissent with respect to those who made an agreement with the government in good faith that the information disclosed about their "private homes" would be kept confidential, particularly those who are yet in possession of the premises involved. What I say does not apply to "public buildings." The words "private homes" and "public buildings" are quoted from the complaint.

I am of opinion that the statute does not require blanket disclosure, to complete strangers, of information which the government obtained under a good faith agreement that it would not be disclosed. For persons who so agreed, I believe the files of information concerning their homes are ". . . similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. 552(b)(6).

There is no question but that giving out this information promiscuously to strangers is an invasion of personal privacy. Disclosure of a specifically agreed upon confidential communication from citizen to sovereign may be considered no less. The question is whether or not it is clearly unwarranted. If the person seeking the information has any colorable interest in obtaining it, I think it may not be the clearly unwarranted invasion contemplated by the statute. These plaintiffs, however, insist that they need have no connection with the premises involved, no matter how remote, in order to get the information sought. Webster's New International Dictionary, 2nd Edition, defines unwarranted as "Not warranted; being without warrant, authority, or guaranty." Plaintiffs' right to interfere, having no interest they have chosen to disclose, is, in my opinion, clearly without warrant or authority, and ought not to be allowed.

With respect to these particular plaintiffs, in their search for information about the private homes of others, I agree with the district court when it stated: "As the House Report accompanying this legislation indicated, a citizen must be able to confide in his Government. When the Government has obligated itself in good faith not to disclose documents or information which it receives, it should be able to honor this obligation."

JULIUS G. GETMAN ET AL.

v.

NATIONAL LABOR RELATIONS BOARD, *Appellant*

No. 71-1097

UNITED STATES COURT OF APPEALS, DISTRICT OF COLUMBIA CIRCUIT

ARGUED JUNE 15, 1971—DECIDED AUG. 31, 1971

Action by law professors engaged in NLRB voting study to compel National Labor Relations Board to provide them with names and addresses of employees eligible to vote in certain elections. The United States District Court for the District of Columbia, Waddy, J., granted relief and th eBoard appealed. The Court of Appeals, J. Skelly Wright, Circuit Judge, held that even if lists constituted "files" within Freedom of Information Act exemption in favor of files disclosure of which would contitute unwarranted invasion of personal privacy, invasion would be minimal, since named employees would only be called by telephone to learn if they would submit to interview, and invasion was not clearly unwarranted, despite claim that it might interfere with and delay determination of elections, particularly since goal of study was streamlining of election process.

Affirmed.

MACKINNON, Circuit Judge, concurred and filed opinion.

1. Records ⇐ 14

Freedom of Information Act exemption in case of trade secrets and commercial orfinancial information obtained from person and privileged or confidential does not extend to any information given government in confidence. 5 U.S.C.A. § 552(b)(4).

2. Records ⇐ 14

Bare lists of names and addresses of employees, which employers were required by la wto give to National Labor Relations Board, without any express promise of confidentiality, were not within Freedom of Information Act exemption applicable to trade secrets and commercial or financial information obtained from person and privileged or confidential. 5 U.S.C.A. § 552(b)(4).

3. Constitutiona Law ⇐ 70(1)

Court was not free to give statute expansion which Congress considered and denied.

4. Statutes ⇐ 217.3

Senate report was to be perferred over House report as reliable indication of legislative intent where House report was not published until after Senate had already passed its bill.

5. Records ⇐ 14

Bare lists of names and addresses of employees which employers were required by law to give NLRB were not within Freedom of Information Act exemption applicable to investigatory files compiled for law enforcement purposes. 5 U.S.C.A. § 552(b)(7).

6. Records ⇐ 14

Freedom of Information Act exemption applicable to personnel and medical files and similar files disclosure of which would constitute clearly unwarranted invasion of personal privacy requires court reviewing matter de novo to balance right of privacy of affected individuals against right of public to be informed, tilting balance in favor of disclosure. 5 U.S.C.A. § 552(b)(6).

7. Records ⇐ 14

Even if disclosure, to law professors engaged in NLRB voting study, of lists of names and addresses of employees, in certain cases, which employers were required to give Board, would be of "files" within Freedom of Information Act exemption in favor of files disclosure of which would constitute unwarranted invasion of personal privacy, invasion would be minimal, since named employees would only be called by telephone to learn if they would submit to interview, and

invasion was not clearly unwarranted, despite claim that it might interfere with and delay determination of elections, particularly since goal of study was streamlining of election process. 5 U.S.C.A. § 552(b)(6).

8. Records ⟸ 14

Court has no equitable jurisdiction under Freedom of Information Act to deny disclosure on grounds other than those laid out under enumerated exemptions, and requirement of balancing applies only to exemption applicable to files disclosure of which would constitute clearly unwarranted invasion of personal privacy. 5 U.S.C.A. § 552(a)(3), (b)(4, 6, 7).

Mr. Norton J. Come, Asst. Gen. Counsel, National Labor Relations Board, with whom Messrs. Arnold Ordman, Gen. Counsel, Dominick L. Manoli, Associate Gen. Counsel, Marcel Mallet-Prevost, Asst. Gen. Counsel, Glen M. Bendixsen, Chief of Special Litigation, and Charles N. Steele, Atty., National Labor Relations Board, were on the brief, for appellant.

Messrs. Stephen B. Goldberg, Champaign, Ill., and Julius G. Getman, Bloomington, Ind., with whom Mr. Lee M. Modjeska, Washington, D.C., was on the brief, for appellees.

Mr. Marvin M. Karpatkin, New York City, for Consumers Union of United States, Inc., as amicus curiae.

Before WRIGHT, MACKINNON and ROBB, Circuit Judges.

J. SKELLY WRIGHT, Circuit Judge.

This case is before the court o nappeal by the National Labor Relations Board from a judgment of the District Court ordering the Board to "provide [appellees] with names and addresses of employees eligible to vote in approximately 35 elections to be designated by [appellees], as soon as those names and addresses are in [the Board's] possession." Although the immediate controversy arises in a labor law context, the central decisional issue involves the right to and limits on disclosure of Government information under the Freedom of Information Act.[1]

I

The history of this action begins with a request by appellees on October 28, 1969 that the Board furnish them the names and home addresses of employees eligible to vote in certain representation elections. The Board now maintains lists of such names and addresses pursuant to its decision in Excelsior Underwear, Inc., 156 NLRB 1236 (1966),[2] to assure that unions have a fair chance to communicate with employees before elections and to facilitate the Board's function of resolving challenges to voter eligibility. Appellees, who are professors of labor law engaged in an NLRB voting study, seek a limited number of *Excelsior* lists in the Board's possession to facilitate scheduling of interviews with employees before and after certain elections. Appellees propose to question willing employees regarding their attitudes toward the election process, especially about the impact of campaign tactics utilized by both employers and unions. On the basis of general statutory authority, the Board has developed an elaborate structure of rules governing the behavior of parties during a campaign. The purpose of appellees' study is to provide an empirical basis for evaluating the wisdom and utility of these regulations.

On April 22, 1970, the Board denied appellees' request for the *Excelsior* lists because, in its judgment, their proposed study would be likely to upset the "laboratory conditions"[3] required for conducting a fair representation election. Even if the proposed interviews would not actually prejudice elections, the Board feared that it would be obliged to conduct investigations and hold hearings concerning interview-related objections, and that this delay would be in disregard of the congressional policy embodied in the National Labor Relations Act that representation issues should be resolved as rapidly as possible.

---

[1] Pub. L. 89-487, 89th Cong., 2d Sess., 80 Stat. 250, 5 U.S.C. § 552 (Supp. II 1965-66), *amending* Administrative Procedure Act, ch. 324, § 3, 60 Stat. 238 (1946), 5 U.S.C. § 1002 (1964). Although Pub. L. 89-487 was repealed, its substantive provisions were enacted into the United States Code by Pub. L. 90-23, 90th Cong., 1st Sess., 81 Stat. 54 (1967), 5 U.S.C. § 552 (1970). For commentaries on the Act, *see* H.R. Rep. 1497, 89th Cong., 2d Sess. (1966) (hereinafter "H. Rep."); S. Rep. 813, 89th Cong., 1st Sess. (1965) (hereinafter "S. Rep."); Dept. of Justice, Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act (1967); K. Davis, Administrative Law Treatise ch. 3A (1970 Supp.); Note, The 1966 Freedom of Information Act—Early Judicial Interpretations, 44 Wash. L. Rev. 641 (1969); Comment, The Freedom of Information Act: Access to Law, 36 Fordham L. Rev. 765 (1968).

[2] Approved in NLRB v. Wyman-Gordon Co., 394 U.S. 759, 767, 89 S. Ct. 1426, 22 L. Ed. 2d 709 (1969).

[3] Sewell Manufacturing Co., 138 NLRB 66, 69-70 (1962).

On August 6, 1970, appellees filed the instant suit in the District Court alleging that they are entitled to the *Excelsior* lists under the Freedom of Information Act. The Board argued that the Freedom of Information Act does not require it to furnish the information sought by appellees because such information falls within Exemptions (4), (6) and (7) of the Act. Cross-motions for summary judgment were filed, and the District Court found on January 21, 1971 that the Board had failed to satisfy its burden of establishing that the requested information was exempted. The District Court further found that, even assuming it had power to deny disclosure on grounds other than those set out in the specific exemptions of the Act, the burden of justifying nondisclosure still rested with the Board, and this burden had not been met. Accordingly, the District Court granted appellees' motion for summary judgment, and the Board brought the appeal which is now before us for consideration.[4]

For the reasons elaborated below, we agree with the District Court that the Board's refusal to disclose the information requested by appellees is not justified under any of the specific exemptions of the Freedom of Information Act. We hold further that a District Court has no equitable jurisdiction to permit withholding of information which does not fall within one of the exemptions of the Act. Accordingly, we affirm the judgment of the District Court.

II

The primary purpose of the Freedom of Information Act is "to increase the citizen's access to government records. * * *

"* * * The legislative plan creates a liberal disclosure requirement, limited only by specific exemptions which are to be narrowly construed. * * * "

Bristol-Myers Co. v. F.T.C., 138 U.S. App. D.C. 22, 25, 424 F.2d 935, 938 (1970).[5] (Footnotes omitted.) Subsection (a)(3) of the Act provides in pertinent part that "each agency, on request for identifiable records * * *, shall make the records promptly available to any person. On complaint, [a] district court of the United States * * * has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complain[ant]. In such a case the court shall determine the matter de novo and the burden is on the agency to sustain its action. * * * "

Subsection (b) of the Act exempts from disclosure nine categories of information. The Board relies on the following three to preclude disclosure in this case:

"(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

* * * * * *

"(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

"(7) investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency[.]"

[1–3] Of the three exemptions relied upon by the Board, Exemptions (4) and (7) are simply inapplicable. The Board, citing the Attorney General's memorandum,[6] maintains that Exemption (4) applies to any information given the Government in confidence. But this interpretation tortures the plain meaning of Exemption (4). We agree with the court in Consumers Union of the United States, Inc. v. Veterans Administration, S.D. N.Y., 301 F.Supp. 796, 802 (1969), that "this section exempts only (1) trade secrets and (2) information which is (a) commercial or financial, (b) obtained from a person, and (c) privileged or confidential. The exemption given by the Congress does not apply to information which does not satisfy the three requirements stated in the statute." [7] Obviously,

---

[4] On January 22, 1971, the Board filed a notice of appeal and asked the District Court to stay its judgment pending appeal. The District Court denied the requested stay on February 8, 1971. On February 9 the Board petitioned this court for a stay pending appeal, which stay was granted on March 11 and dissolved on July 13.

[5] *See also* 112 Cong. Rec. (Part 10) 13641 (1966) (Congressman Moss); 112 Cong. Rec. (Part 10) at 13653 (Congressman Rumsfeld); 111 Cong. Rec. (Part 3) 2797 (1965) (Senator Long of Missouri).

[6] *Supra* Note 1, at 32–34.

[7] *See also* Grumman Aircraft Engineering Corp. v. Renegotiation Board, 138 U.S. App. D.C. 147, 151, 425 F. 2d 578, 582 (1970); K. Davis, *supra* Note 1, § 3A.19. *But see* Barceloneta Shoe Corp. v. Compton, D.P.R., 271 F. Supp. 591 (1967). We note further that, when Congress was considering the Act, the Board took the position that "[t]he phrase 'commercial or financial' unnecessarily limits this exception." Statement of William Feldesman, NLRB Solicitor, in Hearings on S. 1160 Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, 89th Cong., 1st Sess., 490 (1965) (hereinafter "Senate Hearings"). The Board proposed broadening language which was not accepted. We are not free to give Exemption (4) an expansion which Congress considered and denied.

a bare list of names and addresses of employees which employers are required by law to give the Board, without any express promise of confidentiality, and which cannot be fairly characterized as "trade secrets" or "financial" or "commercial" information is not exempted from disclosure by Subsection (b)(4).

[4, 5] Nor is the Board's refusal to disclose justified by Exemption (7), which covers "investigatory files compiled for law enforcement purposes except to the extent available by law to a [private] party." According to Senate Report No. 813 on S. 1160, 89th Cong., 1st Sess., at 9 (1965), "These are the files prepared by Government agencies to prosecute law violators." Their disclosure of such files, except to the extent they are available by law to a private party, could harm the Government's case in court." The *Excelsior* lists are not files prepared primarily or even secondarily to prosecute law violators, and even if they ever were to be used for law enforcement purposes, it is impossible to imagine how their disclosure could prejudice the Government's case in court. Even if this court had not held that specific exemptions from disclosure in the Act are to be narrowly construed, [8] on a simple reading of the plain language of Subsection (b)(7) we would be constrained to hlod that it provides appellant no justification for its withholding of the *Excelsior* lists sought by appellees.

[6] Although Exemption (6) differs from Exemptions (4) and (7) in that it covers information similar in some respects to the kind being sought in this case, we agree with the District Court that the Board has not met the burden of proof required to justify a refusal to disclose under this part of the Act. Exemption (6) applies to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Assuming that the *Excelsior* lists may be characterized as "personnel and medical files and similar files," it is still only a disclosure constituting a "clearly unwarranted invasion of personal privacy" that falls within the scope of Exemption (6). Exemption (6) requires a court reviewing the matter *de novo* to balance the right of privacy of affected individuals against the right of the public to be informed [10]; and the statutory language "clearly unwarranted" instructs the court to tilt the balance in favor of disclosure.[11]

[7] In carrying out the balancing of interests required by Exemption (6), our first inquiry is whether disclosure of the names and addresses of employees constitutes an invasion of privacy and, if so, how serious an invasion. We find

---

[8] *See also* H. Rep. at 11, which is characteristically broader and goes beyond the express terms of the statute. In such instances, we agree with the two District Courts which have considered the issue that the Senate report is to be preferred over the House report as a reliable indication of legislative intent because the House report was not published until after the Senate had already passed its bill. Benson v. General Services Administration, W.D. Wash., 289 F. Supp. 590, 595 (1968), affirmed on other grounds, 9 Cir., 415 F. 2d 878 (1969); Consumers Union of United States, Inc. v. Veterans Administration, S.D.N.Y., 301 F. Supp. 796, 801 (1969), appeal dismissed as moot, 2 Cir., 436 F. 2d 1363 (1971); K. Davis, *supra* Note 1, §§ 3A.2 and 3A.23.

[9] Bristol-Myers Co. v. F.T.C., 138 U.S. App. D.C. 22, 424 F. 2d 935 (1970).

[10] Any discretionary balancing of competing interests will necessarily be inconsistent with the purpose of the Act to give agencies, and courts as well, definitive guidelines in setting information policies. *See* text at page 679 *infra*. But Exemption (6), by its explicit language, calls for such balancing and must therefore be viewed as an exception to the general thrust of the Act. S. Rep., at 9, explains: "The phrase 'clearly unwarranted invasion of personal privacy' enunciates a policy that will involve a balancing of interests between the protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information. The application of this policy should lend itself particularly to those Government agencies where persons are required to submit vast amounts of personal data usually for limited purposes. * * *"

We note in passing that no other exemption specifically requires balancing. In view of the Act's basic purpose to limit discretion and encourage disclosure, we believe that Exemption (6) should be treated as unique, and that equitable discretion should not be imported into any of the other exemptions. *But see* General Services Administration v. Benson, *supra* Note 8, 415 F. 2d at 880, *and* American Mail Line, Ltd. v. Gulick, 133 U.S. App. D.C. 382, 389 and n. 15, 411 F. 2d 696, 703 and n. 15 (1969).

[11] S. Rep. at 9; H. Rep. at 1. The legislative history suggests that use of the "clearly unwarranted" standard is the expression of a carefully considered congressional policy favoring disclosure. At the hearings on the bill various agency spokesmen urged deletion of either the word "clearly" or the entire "clearly unwarranted" phrase so that nondisclosure would have been permitted whenever disclosure would result in any invasion of privacy. *See, e.g.,* testimony of Edwin Rains, Assistant General Counsel, Treasury Department, Senate Hearings at 36; testimony of Fred B. Smith, Acting General Counsel, Treasury Department, Hearings Before a Subcommittee of the Committee on Government Operations of the House of Representatives on H.R. 5012 ,89th Cong., 1st Sess., 56 (1965) (hereinafter "House Hearings"); testimony of Clark R. Molenhoff, Vice Chairman, Sigma Delta Chi Committee for Advancement of Freedom of Information, House Hearings at 151; testimony of William Feldesman, NLRB Solicitor, Senate Hearings at 491 and House Hearings at 257. Congress, however, refused to delete language it considered critical in limiting the scope of the exemption. *See* S. Rep. at 9; H. Rep. at 11.

that, although a limited number of employees will suffer an invasion of privacy in losing their anonymity and in being asked over the telephone if they would be willing to be interviewed [12] in connection with the voting study, the loss of privacy resulting from this particular disclosure should be characterized as relatively minor. Both the House and Senate reports on the bill which became the Freedom of Information Act indicate that the real thrust of Exemption (6) is to guard against unnecessary disclosure of files of such agencies as the Veterans Administration or the Welfare Department or Selective Service or Bureau of Prisons, which would contain "intimate details" [13] of a "highly personal" [14] nature. The giving of names and addresses is a very much lower degree of disclosure; in themselves a bare name and address give no information about an individual which is embarrassing. In the conduct of appellees' study, any disclosure of information more personal than a name and address is wholly consensual and within the control of the employee. Appellees represent that any employee who does not wish to undergo an interview may refuse, and that employees have in fact done so in connection with the pilot studies conducted to date. Although four pilot studies had been conducted at the time briefs were submitted, there is no indication whatever in the record of any harassment of employees who declined to cooperate. Thus assuming *arguendo* that the disclosure of *Excelsior* lists constitutes disclosure of a "file" within the meaning of Exemption (6), and while recognizing that such disclosure does involve some invasion of privacy, we find that the invasion itself is to a very minimal degree.

In determining whether this relatively minor invasion of privacy is "clearly unwarranted," we must also weigh the public interest purpose of appellees' NLRB voting study, the quality of the study itself, and the possibility that appellees could pursue their study without the *Excelsior lists*. As previously indicated, the Board has established complicated rules and enforcement procedures governing the behavior of the parties during election campaigns. The costs of Board regulation are great. The proportion of elections in which the losing party has filed objections has risen to almost one in seven in recent years,[15] and such objections require expensive and time consuming investigation, hearings and rulings. Interference with the "laboratory conditions" required to conduct these elections may indeed result in elections being set aside, as the Board contends. But there is no proof to support the contention. It will be time enough to consider the relief to which the Board is entitled if and when a showing of disruption of Board functions is made.

We agree with appellees that it is ironic that the Board should attempt to use speculation about added delays in the prompt resolution of questions of representation as a basis for preventing this study. One of the primary goals of the study is to consider the feasibility of changing Board rules to eliminate unnecessary grounds for challenges to elections, so as to streamline the entire process. Thus the Board is taking a too shortsighted view of its own self interest. Moreover, the Board's position suffers from the obvious self-justifying tendency of an institution which in over 30 years has itself never engaged in the kind of much needed systematic empirical effort to determine the dynamics of an election campaign or the type of conduct which actually has a coercive impact.[16] The public interest need for such an empirical investigation into the assumptions underlying the Board's regulation of campaign tactics has for some time been recognized by labor law scholars.[17] This particular study has been reviewed and supported by virtually every major scholar in the labor law field.[18] The record is

---

[12] Before attempting to interview a particular employee, appellees first telephone to describe the study and ask if the employee is willing to be interviewed.

[13] H. Rep. at 11.

[14] S. Rep. at 9.

[15] Samoff, NLRB Elections: Certainty and Uncertainty, 117 U. Pa. L. Rev. 228, 253 (1968).

[16] For example, in the 33rd Annual Report of the National Labor Relations Board at 60 (1969) it is stated: "* * * In evaluating the interference resulting from specific conduct, the Board does not attempt to assess its actual effect on the employees, but rather concerns itself with whether it is reasonable to conclude that the conduct tended to prevent the free formation and expression of the employees' choice. * * *" *See also* Murray Envelope Corp. of Mississippi, 130 NLRB 1574, 1576 (1961); Lane Drug Stores, Inc., 88 NLRB 584, 585 n. 5 (1950); Marshall Field & Co., 34 NLRB 1, 10 (1941).

[17] Bernstein, The NLRB's Adjudication-Rule Making Dilemma Under the Administrative Procedure Act, 79 Yale L.J. 571, 582 (1970); *see also* Bok, The Regulation of Campaign Tactics in Representation Elections Under the National Labor Relations Act, 78 Harv. L. Rev. 38, 46–53, 88–90 (1964); Samoff, *supra* Note 13; Note, Behavioral and Non-Behavioral Approaches to NLRB Representation Cases, 45 Indiana L.J. 276 (1970).

[18] *See, e.g.*, Joint Appendix 24, Exhibit 8; JA 25, Ex. 9; JA 26, Ex. 10; JA 15, Ex. 1.

also replete with testimonials from leading management and union representatives and Government officials.[19] Appellees' research has also been approved by the prestigious National Science Foundation, which has awarded appellees the largest grant ever made available for law related research.[20]

Without reviewing the practical workings of the NLRB voting study in detail here, the court notes that appellees Getman and Goldberg are both highly qualified specialists in labor law,[21] that they have designed their study carefully and in collaboration with scholars in the field of survey research over the past two years, and that they have selected and trained their interviewers carefully to avoid biasing effects in the questioning process. The interview part of the study has been tested in three pilot elections and evaluation reveals no evidence which would support the Board's fears that the interviewing might have the effect of confusing or inhibiting the employees. According to the uncontested statement of appellees, no employee who has consented to an initial interview has yet declined to schedule a second interview or to vote in the subsequent election. No employee has brought a complaint concerning the study to either appellees or the Board. Followup checks have shown that employees have been answering truthfully such "sensitive" questions as whether they signed a union authorization card and how they voted.

In striking the balance necessary to determine whether disclosure of the *Excelsior* lists would constitute a clearly unwarranted invasion of privacy, it is also significant that appellees are asking for the names and addresses of employees in only 35 out of the approximately 15,000 elections which the Board will supervise during the next two years [22] and that appellees have no other source for obtaining the names and addresses consistent with their goal of an unbiased and successful study. In each of the pilot studies to date, appellees have obtained a list of employees from the union. But this procedure suffers from the difficulty in persuading the union to give up such lists, which problem has lately been exacerbated because of union fear that the employer involved will emphasize union cooperation with appellees as a tactic in its own campaign. In addition, the Board has asserted that if it is successful in this litigation it might seek to enjoin appellees from carrying out their study, even where the information is obtained from union or management, for the same reason advanced here: that the study will conflict with its responsibility to expedite representation elections under Section 9 of the National Labor Relations Act.[23]

Having considered and weighed all of the above factors, we find it impossible to say that disclosure of the *Excelsior* lists would constitute a clearly unwarranted invasion of employee privacy under Exemption (6) of the Freedom of Information Act.[24] If anything, our finding is that disclosure for purposes of appellees' study is clearly warranted. The invasion of employee privacy strikes us as very minimal, and the possible detrimental effects of the study in terms of

---

[19] *See, e.g.*, JA 31, Ex. 15; JA 34, Ex. 16; JA 35, Ex. 17; JA 28, Ex. 12; JA 29, Ex. 13; JA 30, Ex. 14; JA 19, Ex. 4; JA 15, Ex. 1.

[20] JA 18, Ex. 3.

[21] Professor Getman has taught labor law for eight years and has written several articles concerning the National Labor Relations Act. *See* The Midwest Piping Doctrine: An Example of the Need for Reappraisal of Labor Board Dogma, 31 U. Chi. L. Rev. 292 (1964); Section 8(a)(3) of the NLRA and the Effort to Insulate Employee Free Choice, 32 U. Chi. L. Rev. 735 (1964); The Protection of Economic Pressure by Section 7 of the NLRA, 115 U. Pa. L. Rev. 1195 (1967). Professor Goldberg has taught labor law for six years. His writings include District Court Review of NLRB Representation Elections, 42 Indiana L.J. 455 (1967); The Labor Law Obligations of a Successor Employer, 63 Nw. U.L. Rev. 735 (1969); Coordinated Bargaining Tactics of Unions, 54 Cornell L. Rev. 897 (1969). Both appellees were previously employed as attorneys by the NLRB.

[22] *See* 33rd Annual Report of the National Labor Relations Board, *supra* Note 16, at 1.

[23] 29 U.S.C. § 159 (1964).

[24] This decision, of course, goes only to the merits of appellees' request for disclosure. Although one of the purposes of the 1967 Freedom of Information Act was to limit agency discretion not to disclose by abandoning the former ground rule that a person requesting information show he was "properly and directly concerned," and by instead warranting disclosure to "any person," we find that this purpose is in unavoidable conflict with the explicit balancing requirement of Exemption (6). *See* Note 10 *supra*. Since Exemption (6) necessarily requires the court to balance a public interest purpose for disclosure of personal information against the potential invasion of individual privacy, a court's decision to grant disclosure under Exemption (6) carrries with it an implicit limitation that the information, once disclosed, be used only by the requesting party and only for the public interest purpose upon which the balancing was based. By the same token, our ruling for appellees in this case should not be understood automatically to compel the Board in the future to give out *Excelsior* lists to all other applicants, and for other elections. A request by less well qualified applicants, or applicants with a less carefully designed or more disruptive study would require a new balancing and might be found to inavove a "clearly unwarranted invasion of personal privacy" which would justify nondisclosure.

delaying the election process as highly speculative. On the other hand, the study holds out an unusual promise. As the National Science Foundation concluded in its Proposal Review Summary and Program Recommendations: "The investigators are among the ablest young labor law professors in the country and both have had considerable practical experience in the work of the National Labor Relations Board. In affiliation with a sophisticated social science survey research organization, they have developed a distinctive effort to test the behavioral basis on which an important body of labor law is founded. A successful project here would serve as a much-needed model to encourage further empirical work to test the behavioral assumptions underlying important laws."—JA 164, Ex. 44.

III

[8] Having found that nondisclosure of the *Excelsior* lists is not warranted under Exemption (4), (6) or (7), we must still resolve the question whether the courts have equitable discretion to permit withholding of information which does not fall within one of the specific exemptions to the Act. The District Court in this case held that, "[a]ssuming that [a District Court], in an action under the Freedom of Information Act, may deny disclosure on grounds other than those set out in the specific exemptions to the Act, the burden of justifying non-disclosure must still rest upon the agency. I find that the Board has not met that burden." We do not need to reach the balancing issue decided by the District Court because we agree with the dicta of the panel in Soucie v. David, —— U.S.App.D.C. ——, 448 F.2d 1067 (decided April 13, 1971), and with the Fourth Circuit's decision in Wellford v. Hardin, 444 F.2d 21 (1971), that a District Court has no equitable jurisdiction to deny disclosure on grounds other than those laid out under one of the Act's enumerated exemptions.[25]

In order to appreciate the significance of the relevant language of 5 U.S.C. § 552, one should remember that, prior to the enactment of the Freedom of Information Act in 1966, Section 3 of the Administrative Procedure Act allowed the Government to withhold information "in the public interest" or "for good cause found" and to require the person requesting information to show that he

---

[25] Consumers Union of United States, Inc. v. Veterans Administration, *supra* Note 8, holds that, even where information is not specifically exempted under the Act, the court must still apply "traditional equitable principles." However, counsel for Consumers Union as *amicus curiae* in the instant case was counsel for plaintiff in *Consumers Union* and has brought to our attention the fact that the equitable discretion issue was neither briefed nor argued by either party before the District Court. An unusual set of developments then precluded the District Court's opinion from receiving substantive review on appeal. The scenario was briefly as follows: Consumers Union sought to obtain information the Veterans Administration had compiled in its program to test hearing aids for distribution to veterans. The District Court ordered the VA to disclose the test data, but denied Consumers Union's request for an injunction ordering the VA to disclose comparative scores and the scoring scheme itself, on the theory that such information might confuse and mislead the public and that, even where the Freedom of Information Act permitted disclosure, the District Court possessed discretion to deny remedies where the release of information would result in harm to the public interest. Consumers Union appealed on this point, and the VA cross-appealed on the ground that nondisclosure was protected under some of the specific exemptions of the Act. Subsequent to the decision of the District Court but before oral argument on appeal, the VA made a policy decision to disclose all three types of information originally sought by Consumers Union and actually disseminated this information. The policy was made retroactive to cover contract year 1968, the year for which Consumers Union had solicited information, and Consumers Union was provided with the information it sought in the District Court. The Government then moved to dismiss the appeal as moot. The appellate court denied this motion because the Government's position on cross-appeal suggested that it felt the disclosure was discretionary on its part and not required by the Freedom of Information Act, creating the distinct possibility that the dispute that generated the present action would recur. However, at oral argument the Government dropped its cross-claim and conceded that the results of the tests on hearing aids did not come within any of the exemptions to the Act and that no public interest rationale justified withholding of the information. Under these circumstances, it being quite clear that the Government would not again assert that hearing aid tests are outside the Act or should be concealed in the public interest, the appeal was dismissed as moot. 436 F. 2d 1363.

The Board maintains at page 16 of its brief, citing General Services Administration v. Benson, *supra* Note 8, 415 F. 2d at 880, that the Ninth Circuit has also held that equitable discretion lies to deny disclosure even though none of the exemptions of the Act are applicable. Despite some ambiguous dicta, however, a reading of *Benson* shows that the court made only the much more limited holding that, in determining whether the fifth exemption under the Act is applicable, the court must weigh the effect on the public interest in accordance with traditional equity principles. *See, e.g.*, American Mail Line, Ltd. v. Gulick, *supra* Note 10, 133 U.S. App. D.C. at 389 and n. 15, 411 F. 2d at 703 and n. 15. In fact, Epstein v. Resor, 9 Cir., 421 F. 2d 930, 932–933, cert. denied, 398 U.S. 965, 90 S. Ct. 2176, 26 L. Ed. 2d 549 (1970) suggests that the Ninth Circuit would agree with this court's and the Fourth Circuit's interpretation of the Act.

was "properly and directly concerned." [26] Under the old APA, Section 3, agency and department heads enjoyed a "sort of personal ownership of news about their units," [27] and a wide ranging discretion to suppress information, which was fiercely objected to by the press and other concerned individuals.[28] As a result of this criticism, Congress amended the APA in 1966. The basic purpose of the amendment, which has become popularly known as the Freedom of Information Act, was to guarantee public access to Government information by converting a "withholding" statute to a "disclosure" statute [29] and by mandating full public access to Government information, subject to a limited number of clearly drawn exemptions.[30]

The question whether the courts retain equitable discretion under the Act is settled for us by the express language of the Act, aided by the gloss from the Senate report. Section 552(c) states:

> "This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. * * *" [31]

The Senate report states:

> "The purpose of [§ 552(c)] is to make it clear beyond doubt that all *materials* of the Government are to be made available to the public by publication or otherwise unless explicitly allowed to be kept secret by one of the exemptions in [§ 552(b)]. * * *"

S. Rep. at 10. (Emphasis in original.) The Senate report also sets out that:

> "It is the purpose of the present bill to eliminate such phrases [as 'requiring secrecy in the public interest,' or 'required for good cause to be held confidential'], to establish a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language and to provide a court procedure by which citizens and the press may obtain information wrongfully withheld. It is important and necessary that the present void be filled. It is essential that agency personnel, *and the courts as well*, be given definitive guidelines in setting information policies. * * *"

Id. at 3.[32] (Emphasis added.) We agree with the *Soucie* panel that:

> "* * * Congress clearly has the power to eliminate ordinary discretionary barriers to injunctive relief, and we believe that Congress intended to do so here.
>
> "* * * Through the general disclosure requirement and specific exemptions, the Act thus strikes a balance among factors which would ordinarily be deemed relevant to the exercise of equitable discretion, *i.e.*, the public interest in freedom of information and countervailing public and private interests in secrecy. Since judicial use of traditional equitable principles to prevent disclosure would upset this legislative resolution of conflicting

---

[26] 5 U.S.C. § 1002 (1964), Revised Statutes and Statutes at Large, June 11, 1946, ch. 324, § 3, 60 Stat. 238.

[27] H. Rep. at 2.

[28] *See, e.g.*, Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committte on S. 1666 and S. 1663, 88th Cong., 1st Sess., 7, 16, 35, 60, 82, 95, 140, 237, 27, and 109 (1963).

[29] S. Rep. at 5.

[30] S. Rep. at 3.

[31] As a noted administrative law scholar has observed, "The pull of the word 'specifically' is toward emphasis on statutory language and away from all else—away from implied meanings, away from reliance on legislative history, away from needed judicial legislation." K. Davis, *supra* Note 1, § 3A.15. Finding the statute to be badly drafted and in some instances ill conceived, Professor Davis suggests that the courts might act to redraft the statute by invoking the doctrine of equitable discretion. *See, e.g.*, §§ 3A.1, 3A.16, and 3A.19. We decline this course. If the courts began to invoke their equitable powers to permit nondisclosure running beyond the enumerated exemptions of § 552(b), the overriding purpose of the Act—which is to require disclosure in all but a narrowly and clearly defined category of situations—would be seriously undermined.

[32] The House report differs from the Senate report in that is suggests that District Courts may have equitable discretion. *E.g.*, "[t]he Court will have authority whenever it considers such action equitable and appropriate to enjoin the agency from withholding its records and to order the production of agency records improperly held." H. Rep. at 9. And "[t]he purpose of this subsection is to make clear beyond doubt that all the materials of Government are to be available to the public unless specifically exempt from disclosure by the provisions of subsection (e) [§ 552(b)] *or limitations spelled out in earlier subsections.*" *Id.* at 11. (Emphasis added.) For the reasons set out in Note 8 *supra*, however, we consider the Senate report the more reliable indicator of legislative intent.

interests, we are persuaded that Congress did not intend to confer on district courts a general power to deny relief on equitable grounds apart from exemptions in the Act itself. * * *"

—— U.S. App. D.C. at ——, 448 F. 2d at 1067.

To sum up, the names and addresses of employees are information within the scope of the Freedom of Information Act, which was designed in part to "provide the means by which the people of this country can become informed and thus be able to scrutinize the activities and operation of their Government."[33] While the Board is correct that the *Excelsior* lists are but the first step in the total information gathering process in which appellees are engaged and that the lists themselves do not in any direct sense reveal anything about the Board's operations, there is no language or principle embodied in the Act which requires that information sought under its authority be sufficient, in and of itself, to evaluate the agency's performance. The *Excelsior* lists failing to fall within any of the Act's enumerated exceptions, and there being no equitable discretion in a District Court to create new exemptions, appellees are entitled to disclosure.

Affirmed.

MacKinnon, Circuit Judge (concurring):

The extremely broad sweep of the Freedom of Information Act, with its narrow exemptions, makes it mandatory in my opinion—if we are to follow the directions of Congress—to direct the National Labor Relations Board to furnish appellees with the names and addresses of employees as requested. However, I agree with the Board that this request could lead to undesirable interference in elections. Furnishing these lists for use by third parties *during* the representation election may interject a third factor which really has no place in the election. I cannot say, however, that the release of the lists "would constitute a *clearly unwarranted* invasion of privacy." Whether appellees' interference in these elections will be misunderstood and misinterpreted and will cause adverse reactions is unpredictable at this stage.

My principal concern is for the future. We are here following the dictates of Congress and are making information available for a use that may interfere with the proper functioning of government. This use may have its beneficial effects also, but before the good is harvested considerable turmoil and disruption may result. And this decision is only the beginning. We may expect similar wholesale demands for lists of names and addresses from other persons, not for what they may disclose about the functioning of government, but for their collateral ability to aid the person requesting such information.

While it must be recognized that the Board might return the lists to the employers and in the future might alter its *Excelsior* rule so that employers would deliver the names and addresses to the unions directly rather than filing them with the regional directors, and thus obviate the requirement to disclose, the annoyance to individuals and the Government that could result from requiring the Government to furnish various lists of names and addresses to various persons on request could be very substantial.

It seems to me that furnishing bare lists of names and addresses of various groups of persons in various Government files is not the sort of disclosure that Congress basically had in mind in enacting the Freedom of Information Act. But in my opinion, the Act as it presently exists practically requires the disclosure of such lists on demand. One need not elaborate on the various abuses that could result if lists of people as classified by the Government for particular purposes became available practically on demand in wholesale lots. If this situation is to be corrected, it will require an amendment to the Act.

---

[33] Remarks of Senator Dirksen, 110 Cong. Rec. (Part 13) 17088 (1964). Although the primary purpose of the Act may be to help the citizen to know "how his Government is operating," H. Rep. at 6, we note in passing the Act is not limited to disclosures involving public scrutiny of governmental operations. In Consumers Union of United States, Inc. v. Veterans Administration, *supra* Note 8, the publisher of Consumer Reports obtained certain records of a VA hearing aid testing program for a purpose which had nothing whatever to do with revealing Government operations—it merely wished to advise its readers which hearing aids were best. Similarly, in General Services Administration v. Benson, *supra* Note 8, the plaintiff, who obtained Government records concerning the value of certain property it had sold him, needed those records for the purely personal purpose of substantiating his position in a dispute with the Internal Revenue Service as to the tax consequences of that sale.

OCTOBER TERM, 1971

Opinion in Chambers

NATIONAL LABOR RELATIONS BOARD

v. GETMAN ET AL.

ON APPLICATION FOR STAY

No. A–109. Decided July 27, 1971

Stay of District Court's order under the Freedom of Information Act, 5 U.S.C. § 552 (a)(3), that National Labor Relations Board (NLRB) provide respondents with certain records concerning labor representation elections denied, the Act providing no exception authorizing the NLRB's refusal to produce the requested records.

MR. JUSTICE BLACK, Acting Circuit Justice.

Respondents, two law professors who are undertaking a study of labor representation elections, applied for and obtained an order from the United States District Court for the District of Columbia requiring the National Labor Relations Board to provide respondents "with names and addresses of employees eligible to vote in approximately 35 elections to be designated by (respondents)." Respondents base their claim to the information on the language of the Freedom of Information Act, 5 U.S.C. § 552 (a)(3), which requires that a Government agency "on request for identifiable records . . . shall make the records promptly available to any person." The Government has filed an application seeking a stay of the order of the District Court. This application was assigned to me in the absence of THE CHIEF JUSTICE.

The Government applies for a stay on the ground that the District Court order requiring the Board to comply with the Freedom of Information Act and deliver the records in question to respondents would interfere with the representation election procedures under the National Labor Relations Act, 49 Stat. 449, as amended. The Board was created by Congress and Congress has seen fit to make identifiable records of the Board and other Government agencies available to any person upon proper request. I find no exception in the Freedom of Information Act which would authorize the Board to refuse promptly to turn over the requested records. I deny the application for stay without prejudice to the Government to present its application to another Member of this Court.

It is so ordered.

Appendix D—Expungement of Records

MAX I. CHASTAIN

v.

CLARENCE M. KELLEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, APPELLANT.

No. 73–2137

UNITED STATES COURT OF APPEALS, DISTRICT OF COLUMBIA CIRCUIT

APRIL 2, 1975

After suspension and proposed dismissal of special agent of the FBI was cancelled, the agent filed motion for order requiring the FBI to expunge all records relating to the suspension and proposed dismissal, to refrain from basing any further personnel action on those matters and to inform all agencies to which FBI had disseminated information concerning the incident that the charges had been withdrawn. The United States District Court for the District of Columbia, Oliver Gasch, Jr., granted the motion and the FBI and its director appealed. The Court of Appeals, McGowan, Circuit Judge, held that expungement order was improper

absent finding that information in the records was inaccurate, was acquired by fatally flawed procedures or was prejudicial without serving any proper purpose of the FBI.

Judgment vacated and case remanded with instructions.

Tamm, Circuit Judge, did not participate.

1. Records ⇨ 22

Federal courts are empowered to order the expungement of government records where necessary to vindicate rights secured by the Constitution or by statute.

2. Records ⇨ 22

Power of federal court to order expungement of government records may be invoked even when records in question are administrative rather than criminal

3. Records ⇨ 22

Expungement of government records is an equitable remedy over which trial judge exercises considerable discretion.

4. Records ⇨ 22

Expungement of government records is tool which must be applied with close attention to the peculiar facts of each case.

5. Records ⇨ 22

Order requiring FBI, following cancellation of suspension and proposed dismissal of special agent, to expunge records relating to the matter was improper, absent finding that information contained in the records was inaccurate, was acquired by fatally flawed procedures or was prejudicial to the agent without serving any proper purpose of the FBI.

6. Records ⇨ 22

Even if abandonment of proposed disciplinary action against special agent of the FBI and failure of FBI to file timely motion in opposition to agent's motion for order expunging FBI's records concerning the matter could be presumed to constitute an admission that charges against the agent were inaccurate, improperly made or insignificant, reasonableness of such presumption was destroyed and order of expungement could not be justified on basis of such presumption, where FBI filed subsequent opposition to agent's motion and stated that cancellation of the disciplinary action did not absolve agent of wrongdoing.

7. Records ⇨ 41

FBI had obligation to correct any erroneous information which had been disseminated to other agencies and which concerned matters giving rise to disciplinary proceedings instituted against special agent.

8. Records ⇨ 22

Refusal to grant motion filed by FBI for reconsideration of order expunging records concerning disciplinary action taken against special agent was improper even though FBI's opposition to motion for order of expungment was filed two days late, where trial court was not inconvenienced greatly and order had been entered without hearing on the merits and had effect of removing from agent's personnel file all reference to what appeared to have been a serious want of sound judgment on agent's part in the exercise of his official authority. 44 U.S.C.A. § 3301 et seq.; Fed.Rules Civ.Proc. rules 59(e), 60, 28 U.S.C.A.

Appeal from the United States District Court for the District of Columbia (D.C. Civil Action 570-73).

Barbara L. Herwig, Atty., Dept. of Justice, with whom Irving Jaffe, Acting Asst. Atty. Gen., Earl J. Silbert, U.S. Atty., and Robert E. Kopp, Atty., Dept. of Justice, were on the brief, for appellant. Harold H Titus, Jr., U.S. Atty. at the time the record was filed, John A. Terry and Robert M. Werdig, Jr., Asst. U.S. Attys., also entered appearances for appellant.

Lawrence Speiser, Washington, D.C., for appellee.

Before Fahy, Senior Circuit Judge, and McGowan and Tamm, Circuit Judges.

Opinion for the Court filed by Circuit Judge McGowan.

McGowan, Circuit Judge:

The District Court ordered the Federal Bureau of Investigation to expunge all records of an incident giving rise to charges by it that one of its agents had,

among other things, misused his credentials. After first suspending the agent and giving him notice of proposed dismissal, the Bureau subsequently decided not to take this action. It was two days late in filing an opposition to the motion to expunge, which had been promptly filed after the Bureau's decision and as promptly granted. We think that there are interests at stake going beyond those of the immediate parties to this litigation, and which warrant our vacating the judgment entered by the District Court in order that the Government may be heard on the question of expungement.

I

Plaintiff-appellee became a Special Agent of the FBI in November of 1970. On March 8, 1973, he received a letter from L. Patrick Gray, III, then the Bureau's Acting Director, informing him of his immediate suspension without pay and of his proposed dismissal as of thirty days from the letter's receipt. The letter set out a number of grounds for these actions. They all arose from the circumstances we now summarize.

On January 29, 1973, appellee was on leave from his duties in the Bureau's Washington Field Office, and was spending several days in Virginia Beach, Virginia, his purpose, at least in part, was to visit a femal friend who was married to a naval officer then absent on assignment. Plaintiff had grown intimate with the woman during his own earlier naval service. She informed him upon arrival that another woman, a mutual acquaintance and also a resident of Virginia Beach, had recently complained of receiving a number of obscene telephone calls. Appellee came to the complainant's aid. He went to the home of the neighbor whom she suspected was responsible for the calls. Gaining entrance, he displayed his FBI credentials and asked the neighbor a number of probing questions aimed at discovering whether he was indeed the culprit. The neighbor's mother, who was present at the time, later reported the incident to the local FBI office in Norfolk, Virginia. After the interview, appellee reported back to the recipient of the telephone calls his conclusion that her suspicions about the neighbor were correct. He also divulged the neighbor's true name, which he had discovered during the interview.

For this conduct, which appellee recounts in somewhat more innocuous terms but does not really deny,[1] the Acting Director charged him with misuse of his FBI credentials, unauthorized disclosure (to the complainant about the telephone calls) of investigative information gained through his official position, and failure to inform the Special Agent in charge of the Norfolk office of an investigation within that agent's territory. Appellee was further accused of not having kept his Washington superiors sufficiently informed of his whereabouts (he had left only the post office box number of his female friend) and also of "deception, lack of integrity, [and] uncooperative attitude." The Acting Director gave as an example of the latter the fact that, in the course of applying to become a Special Agent, appellee had responded negatively to the question of whether he had any moral deficiencies, and had not reported the relationship he had had with the female friend during his earlier naval days.

On March 26, 1973, before final action was taken by the Bureau pursuant to its March 8 letter, appellee sued in the District Court for an order prohibiting his dismissal and restoring him to active duty. A temporary restraining order was entered against dismissal only. While appellee's motion for a preliminary injunction was still pending, William Ruckelshaus replaced Gray as the Bureau's Acting Director. Ruckelshaus cancelled the suspension and proposed dismissal, and also awarded plaintiff his back pay. On May 23 the Government moved that the case be dismissed as moot. Appellee moved the following day for an order requiring the FBI (1) to expunge all records relating to the suspension and proposed dismissal, (2) never to base any further personnel action on those matters, and (3) to inform all those agencies to which the FBI had disseminated information about them that the charges had been withdrawn. On June 6 the District

[1] Appellee submitted for *in camera* inspection by the District Court an affidavit in which, *inter alia*, he admitted the investigative visit to the house of the suspect neighbor, but maintained that during it he had been courteous, had displayed his credentials only to put the neighbor at ease, and had specified that his was not an official FBI investigation. App. II at 8–25.

Court dismissed the case as moot, and, no opposition having been filed by the Government, granted the motion for expungement.[2]

II

[1, 2] The federal courts are empowered to order the expungement of Government records where necessary to vindicate rights secured by the Constitution or by statute. *See, e.g.*, Menard v. Saxbe, 162 U.S.App.D.C. 284, 498 F.2d 1017, 1023 (1974); Sullivan v. Murphy, 156 U.S.App.D.C. 28, 478 F.2d 938, 966 (1973); Menard v. Mitchell, 139 U.S.App.D.C. 113, 430 F.2d 486 (1970). The cited cases involved the retention and dissemination of criminal records, and it is in that context that the propriety of expungement orders has been most thoroughly explored. Since the power to order expungement is, however, only an instance of the general power of the federal courts to fashion appropriate remedies to protect important legal rights,[3] it may also be invoked when the Government records in question are administrative rather than criminal.

The precedents in this latter regard are few, but they are clear enough. In Peters v. Hobby, 349 U.S. 331, 75 S.Ct. 790, 99 L.Ed. 1129 (1955), for example, the Supreme Court held that the Loyalty Review Board, an organ of the Civil Service Commission established to review the recommendations of federal agencies that employees be dismissed for disloyalty to the United States, exceeded its jurisdiction in reopening the case of an employee whose loyalty had been approved by the relevant agency. The relief to which the Court found the employee entitled included "an order directing the respondent members of the Civil Service Commission to expunge from its records the Loyalty Review Board's finding that there is a reasonable doubt as to petitioner's loyal . . ." *Id.* at 348–349, 75 S.Ct. at 799.[4]

[3, 4] Expungement, no less than any other equitable remedy, is one over which the trial judge exercises considerable discretion. It is a versatile tool: expungement of only some records, from some Government files, may be enough,

---

[2] The order in its entirety required:

1. That defendant and his successors shall remove from plaintiff's personnel file and from all records of the Federal Bureau of Investigation any and all records, memoranda, documents, writings, statements of witnesses, anad investigative records, describing, referring to or alluding to the facts upon which the suspension and the proposed termination of plaintiff were based; and

2. That defendant and/or his successor or successors are permanently enjoined from using any of the information or records referred to in Paragraph 1 of this Order or any records relating to this suit as criteria for advancement, promotion, salary increase or any other professional award or for any disciplinary action or termination of employment; and

3. That defendant and/or his successor or successors shall contact any and all agencies, including the United States Civil Service Commission, to which they have disseminated any information regarding plaintiff and the facts upon which plaintiff's suspension and proposed termination or this suit were based and inform each such agency that the Bureau had withdrawn the suspension and proposed termination and that this Court has requested each such agency to remove any and all references of the above from any of its records. App. I at 49–50.

[3] *See* Bivens v. Six Unknown Federal Narcotics Agents, 403 U.S. 388, 396, 91 S. Ct. 1999, 29 L. Ed. 2d 619 (1971); Swann v. Board of Education, 402 U.S. 1, 15, 91 S. Ct. 1267, 28 L. Ed. 2d 554 (1971); United States v. McLeod, 385 F. 2d 734, 748–750 (5th Cir. 1967).

[4] *Accord*, Service v. Dulles, 98 U.S. App. D.C. 268, 235 F. 2d 215, 219 (1956) rev'd on other grounds, 354 U.S. 363, 77 S. Ct. 1152, 1 L. Ed. 2d 1403 (1957). *See also* Smith v. District Unemployment Compensation Board, 140 U.S. App. D.C. 361, 435 F. 2d 433, 439 (1970) (Federal agency's finding that ex-employee had resigned without cause, which finding made her ineligible for unemployment compensation, stricken unless required hearing provided). *Cf.* Finley v. Hampton, 154 U.S. App. D.C. 50, 473 F. 2d 180 (1972) (presence in files of federal agency that employee had friends with "homosexual mannerisms" did not constitute cognizable legal injury); Newell v. Ignatius, 132 App. D.C. 252, 407 F. 2d 715 (1969) (suit by naval disenrollee to expunge records of alleged disloyalty mooted by Navy's voluntary expungement).

In Janca v. Gray, Civil No. 1351–71 (D.D.C., filed April 2, 1973), two ex-employees of the FBI alleged that they had been illegally discharged because of their off-hours work for an organization which opposed certain foreign American military involvements. Following a default judgment, the Bureau was ordered, in terms similar to those of the order herein appealed from, to expunge all records of the incident, to base no future personnel action thereon, and to bring the court's order to the attention of all other agencies to which information concerning the incident had been disseminated. An appeal was taken but subsequently abandoned by the Government.

Were it necessary to protect important statutory or constitutional rights of appellee, expungement in this case would not be prevented, as the Government has argued, by the command of 44 U.S.C. § 3314 (1970) that Government records "may not be alienated or destroyed except under this chapter." Since it clearly effects no repeal of other provisions, this general statutory command must be reconciled with other statutory requirements, and must bow to them when they are more specific, as of course it must bow to the Constitution.

as may the placing of restrictions on how the information contained in the records may be used. It is a tool which must be applied with close attention to the peculiar facts of each case. Only in that way can it effect a proper reconciliation of the competing interests of the Government in retaining information relevant to job performance, and of the individual in having it forgotten. But it must be rationally and selectively responsive to those interests.

Appellee's interest is in the vindication of the rights alleged in his complaint, that is to say, in not being (i) suspended without pay during the thirty-day notice period in violation of the Veteran's Preference Act, (ii) suspended or dismissed without such hearing as due process requires, (iii) penalized by one who was serving illegally as the Bureau's Acting Director; or (iv) dismissed for improper or unsubstantiated reasons.[5] These rights, assuming they exist, were in large part vindicated when appellee was reinstated with back pay.

[5] There may remain a right not to be adversely affected by the information in the future. Such a right may exist if the information (1) is inaccurate, (2) was acquired by fatally flawed procedures, or (3) as may be the case with information about his private and personal relationships, is prejudicial without serving any proper purpose of the Bureau's. But there has not as yet been a finding by the trial court that any of these conditions exist. In fact, appellee has made no objection to the manner in which the Bureau carried out its inquiry, and he has admitted the substantial truth of what it found with respect to the misuse of his credentials. Moreover, the Bureau would appear to have a strong interest in retaining at least some of the information that the District Court ordered expunged. The abuse of official power by appellee in this case may seem a mild one, but even mild abuses, should they be tolerated and allowed to proliferate, will pose a severe threat to the public confidence upon which the Bureau relies.

[6] The order may well have been justified at the time it was originally entered. The new Acting Director's abandonment of the proposed disciplinary action could, in one view of the matter, be taken as implying an admission by him that the charges against appellee were inaccurate, improperly made, or simply insignificant. Such an admission might well have justified expungement, and might be presumed to have been made when the time in which to oppose expungement expired without the new Acting Director's raising any objection. The reasonableness of that presumption was destroyed, however, when the Government filed its subsequent opposition, which included the following statements:

> By the cancellation of the proposed dismissal and suspension, plaintiff was not absolved of any wrongdoing. The fact remains plaintiff did misuse his credentials and did unnecessarily involve the FBI in a matter over which it had no jurisdiction.

App. I at 52.

We do not know the precise reason for the cancellation. The new Acting Director may have considered only some of the charges against plaintiff to be credible and proper. Or—and what seems more likely—he may have thought the admitted misconduct insufficient, at least as a first offense, to warrant the severe sanction of dismissal. In any event, his opposition, albeit belated, raised doubts as to the propriety of expungement, and strongly suggested the desirability of a hearing on its merits.

The expungement order must therefore be vacated, and is not to reissue prior to a hearing on the extent to which the information in the Bureau's files violates appellee's rights without serving any legitimate needs of the Bureau. In this connection we note the considerable latitude given the Bureau in its internal affairs, *cf.* Carter v. United States, 132 U.S.App.D.C. 303, 407 F.2d 1238, 1242 (1968), and also the limited relevance of the cases involving expungement of criminal records, the potential prejudicial effects of which far exceed that of the information here at issue. *Compare* Menard v. Saxbe, *supra*, 498 F.2d at 1024 (adverse effects of criminal records enumerated), *with* Finley v. Hampton, 154 U.S.App.D.C. 50, 473 F.2d 180 (1972) (effect of certain adverse information in employing agency's files found not legally cognizable).

[7] The part of the challenged order to which we see least objection is that requiring the Bureau to inform other agencies to which it has hitherto disseminated information about this matter that appellee was not in fact disciplined for it. Certainly it is the Bureau's obligation to correct any erroneous information. Since the action the Board is required to take with respect to other agencies will otherwise depend on what it itself is required to do, however, it seems best

---

[5] App. I at 4–10.

to vacate the entire order and to allow the District Court to reexamine—and perhaps to refashion—it in the light of what may be revealed by further proceedings.

III

The Government has not made it easy for the courts to protect its interest in this case. The challenged order was filed without opposition on June 6. On June 18 the Government moved for reconsideration under Fed.R.Civ.P. 60, but failed to allege any of the grounds upon which reconsideration may be granted thereunder. Instead, it asserted only that the order was "contrary to 44 U.S.C. § 3301 et seq., and the prevailing case law in this jurisdiction." App. I 55. A supporting memorandum incorporated by reference the Government's earlier untimely opposition to expungement, adding a case citation and quotations from 44 U.S.C. § 3301 et seq.[6] Thus, the Government in its reconsideration motion attacked the district judge's order on its merits, apparently assuming that Rule 60 gave it its first opportunity to appeal, which of course it does not. Gilmore v. Hinman, 89 U.S.App.D.C. 165, 191 F.2d 652, 653 (1951).

Perhaps the Government intended, as it now argues it did, to move under Rule 59(e) to alter or amend judgment. Actually the more appropriate motion was indeed under Rule 60.[7] Expungement was ordered, we must assume for present purposes, because it was unopposed; and what the Government needed was to be relieved of this default. Rule 60 allows reconsideration of such a "default judgment" where the failure to oppose is due to "excusable neglect." *See* 7 Moore, Federal Practice 248–251 (1974), and cases cited. As it happened, the Government offered no excuse whatsoever; and, under the circumstances, the district judge's refusal to reconsider was certainly understandable.

[8] It was not, however, required. Reliance on the wrong Rule may be overlooked, as neglect may be excused, in the discretion of the trial judge,[8] and we do not think that that discretion was exercised to the best purpose in this instance. The Government's errors, whether excusable or not, certainly worked no great inconvenience on the court, the opposition to expungement being out of time by only two days. More important, reconsideration was sought of an order on which there had never been a hearing on the merits, and which had the effect of removing from appellee's personnel file all reference to what appears to have been a serious want of sound judgment on his part in the exercise of his official authority.

The latter factor is most persuasive for us. The expungement order on its face appears to flow as a natural consequence from the Bureau's having abandoned its purpose to punish appellee by dismissal. It would indeed be unfortunate if in the future the Bureau were to think that, once it had proposed the suspension and dismissal of an employee, its only choices were to carry out that particular threat or to have all trace of the matter expunged from its records.

To be sure, we could limit the precedential effect of the district judge's decision in this case by upholding it solely on the basis of the Government's procedural oversights. But appellee was by his own admission guilty of "questionable judgment." Should that lapse on his part be wiped from the Bureau's records, it may be at the expense of other agents whose records better qualify them for promotion or other preferment. They should not suffer for the Government's procedural errors, any more than should the public who bear the brunt of such lapses and who are entitled to have the Bureau's personnel administration take them into account.

The judgment appealed from is vacated and the case remanded with instructions to allow the Government an opportunity to be heard in opposition to the motion for expungement in further proceedings consistent with this opinion.

It is so ordered.

TAMM, Circuit Judge, did not participate in the disposition of this case.

---

[6] *See* note 4 *supra* (last paragraph).

[7] It is not as clear as the Government seems to have assumed that a movant under Rule 59(e) may seek to "alter or amend" a judgment simply because it was erroneous. *Cf.* Erickson Tool Co. v. Balas Collet Co., 277 F. Supp. 226, 234 (N.D.Ohio 1967) (not the purpose of Rule 59(e) to allow movant to seek "complete reversal of the Court's judgment"), aff'd 404 F.2d 35 (6th Cir. 1968).

[8] *See* Hutches v. Renfroe, 200 F.2d 337, 341 (5th Cir. 1952); Randolph v. Randolph, 91 U.S.App.D.C. 170, 198 F.2d 956 (1952); 7 Moore Federal Practice 251 (1974).

○

UNIVERSITY OF FLORIDA
3 1262 05621 9248